国盟信息安全通报

2020 年 11 月 22 日第 229 期

全国售后服务中心

国盟信息安全通报

（第 229 期）

国际信息安全学习联盟

2020 年 11 月 22 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 716 个，其中高危漏洞 247 个、中危漏洞 390 个、低危漏洞 79 个。漏洞平均分值为 6.00。本周收录的漏洞中，涉及 0day 漏洞 471 个（占 66%），其中互联网上出现“QEMU OS 命令注入漏洞、Wordpress EZ-done File Manager 远程文件上传漏洞”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 4094 个，与上周（3727 个）环比增加 10%。

主要内容

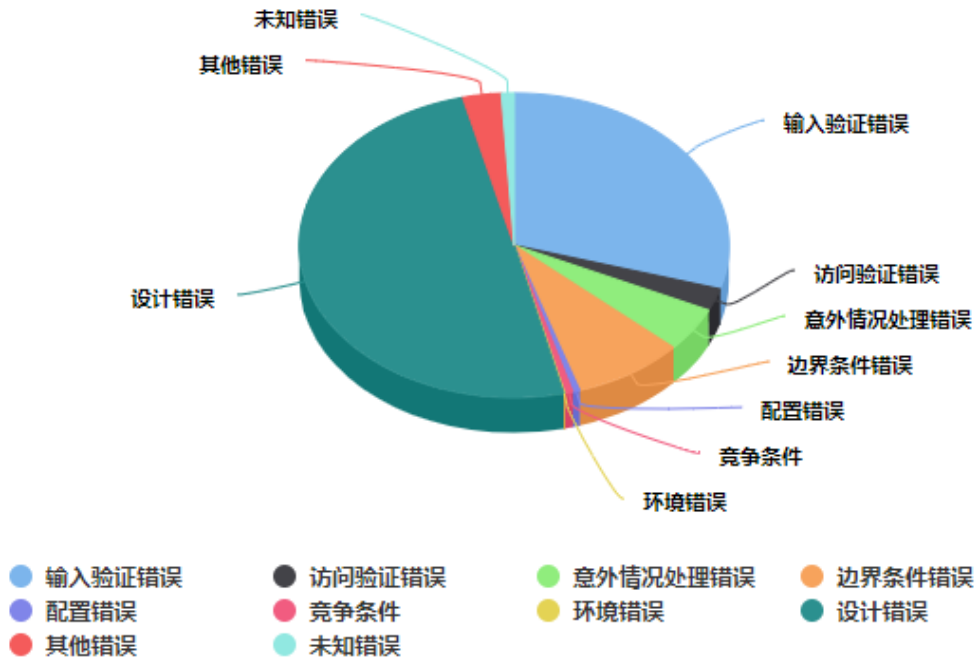
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

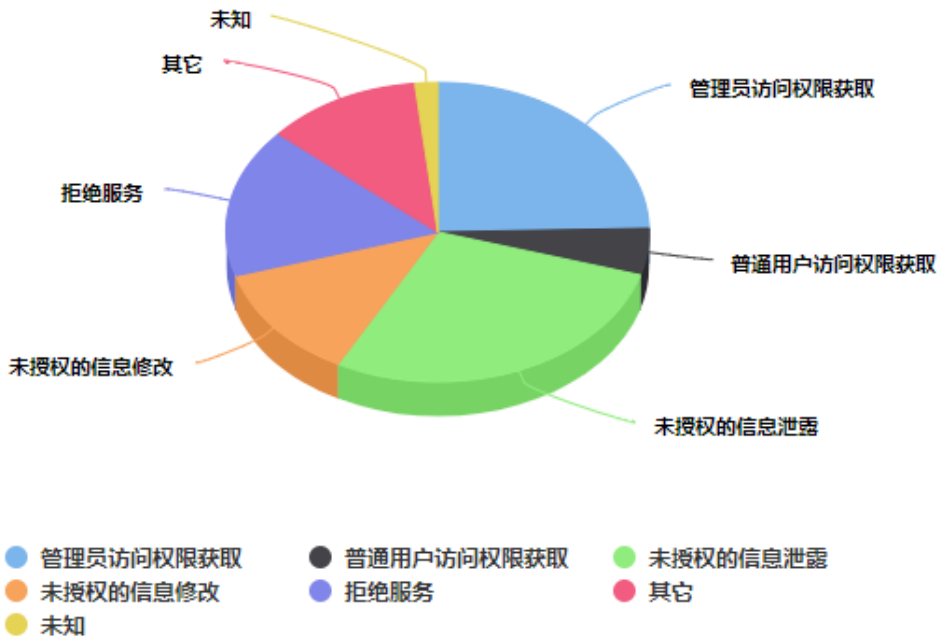
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 716 个，其中高危漏洞 247 个、中危漏洞 390 个、低危漏洞 79 个。漏洞平均分值为 6.00。本周收录的漏洞中，涉及 0day 漏洞 471 个（占 66%），其中互联网上出现“QEMU OS 命令注入漏洞、Wordpress EZ-done File Manager 远程文件上传漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 4094 个，与上周（3727 个）环比增加 10%。

二、安全漏洞增长数量及种类分布情况

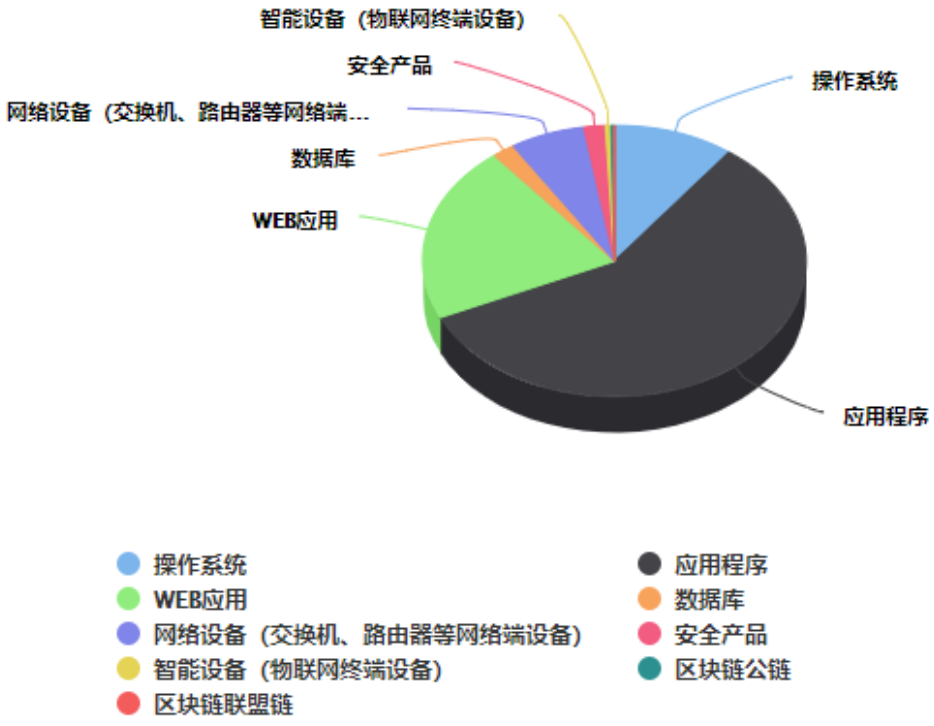
➢ 漏洞产生原因（2020 年 11 月 08 日—2020 年 11 月 22）



➢ 漏洞引发的威胁（2020 年 11 月 08 日—2020 年 11 月 22）



➢ 漏洞影响对象类型（2020 年 11 月 08 日—2020 年 11 月 22）



三、安全产业动态

➢ 世界互联网大会组委会发布《携手构建网络空间命运共同体行动倡议》

2020 年 11 月 18 日，世界互联网大会组委会发布的《携手构建网络空间命运共同体行动倡议》。**以下为全文：**

当今世界正经历百年未有之大变局，新冠肺炎疫情持续蔓延，给世界各国带来严重冲击。国际社会唯有同舟共济、守望相助，才能打赢这场全人类与病毒的战争，走出这段艰难的时刻。面对新的风险和挑战，如何在网络空间加强团结协作、维护公平正义、共享数字红利，成为摆在我们面前的重大课题。

2015 年，中国国家主席习近平在第二届世界互联网大会提出“四项原则”“五点主张”，倡导尊重网络主权，推动构建网络空间命运共同体，为全球互联网发展治理贡献了中国智慧、中国方案。2019 年，第六届世界互联网大会组委会发布《携手构建网络空间命运共同体》概念文件，进一步阐释了这一理念。当前疫情背景下，构建网络空间命运共同体的重要性和紧迫性更加凸显。我们呼吁，各国政府、国际组织、互联网企业、技术社群、社会组织和公民个人坚持共商共建共享的全球治理观，秉持“发展共同推进、安全共同维护、治理共同参与、成果共同分享”的理念，把网络空间建设成为造福全人类的发展共同体、安全共同体、责任共同体、利益共同体。**为此，我们提出以下行动倡议：**

发展共同推进

采取更加积极、包容、协调、普惠的政策，加快全球信息基础设施建设，推动数字经济创新发展，提升公共服务水平。

1.提升互联网接入水平，促进互联互通。推动各国在光缆骨干网、国际海缆等通信基础设施领域开展合作，在尊重各国网络主权、尊重各国网络政策的前提下，探索以可接受的方式扩大互联网接入和连接，让更多发展中国家和人民共享互联网带来的发展机遇。

2.推进信息基础设施建设。携手提升信息基础设施建设、运营与服务水平。支持 5G、物联网、工业互联网建设、应用和发展，打造新的经济增长动能，助力经济恢复与发展。

3.利用信息通信技术提升公共服务水平。推动利用数字技术应对疫情、自然灾害等突发公共事件的经验分享与合作，利用数字技术提升文化教育、环境保护、城市规划、社区管理、医疗健康等公共服务水平。

4.促进数字产业融合与经济转型升级。鼓励数字技术与传统产业融合发展，提升数字化、网络化、智能化水平，促进经济转型升级，推动数据要素的开发利用与共享。

5.创建良好的营商环境，维护全球信息通信产业链供应链开放、稳定、安全。为企业提供开放、公平、非歧视的营商环境，加强团结协作，携手共克时艰，全面提振全球市场信心。推动建立健全多边、互信、共赢的数字产业规则，保障全球信息通信产业链供应链开放、稳定、安全，推动全球经济健康发展。

安全共同维护

倡导开放合作的网络安全理念，坚持安全与发展并重，共同维护网络空间和平与安全。

6.增强网络空间战略互信。鼓励开展全球、区域、多边、双边与多方等各层级的合作与对话，共同维护网络空间和平与稳定，增进各国之间战略互信，反对网络攻击、网络威慑与讹诈，反对利用信息技术从事危害他国安全和社会公共利益的行为，防止网络空间军备竞赛，营造和平的发展环境，防止技术议题政治化。

7.加强信息基础设施保护。加强在预警防范、信息共享、应急响应等方面的合作，积极开展关键信息基础设施保护的经验交流。反对利用信息技术破坏他国关键信息基础设施或窃取重要数据。

8.加强个人信息保护和数据安全管理。规范个人信息收集、存储、使用、加工、传输、提供、公开等行为，保障个人信息安全，开展数据安全和个人信息保护及相关规则、标准的国际交流合作，推动符合《联合国宪章》宗旨的个人信息保护规则标准国际互认。要求企业不得在信息技术设备中预设后门、恶意代码，不得利用提供产品、服务的便利条件窃取用户

数据。

9.加强未成年人网络保护。开展未成年人网络保护立法经验交流，打击针对未成年人的网络犯罪和网络欺凌，保护未成年人网上隐私，培育提高未成年人网络素养，形成健康的上网习惯。

10.深化打击网络犯罪、网络恐怖主义国际合作。对网络犯罪开展生态化、链条化打击整治，进一步完善打击网络犯罪与网络恐怖主义的机制建设。支持并积极参与联合国打击网络犯罪全球性公约谈判。有效协调各国立法和实践，合力应对网络犯罪和网络恐怖主义威胁。

治理共同参与

坚持多边参与、多方参与，加强对话协商，推动构建更加公正合理的全球互联网治理体系。

11.发挥联合国在网络空间国际治理中的主渠道作用。充分发挥联合国信息安全开放式工作组（OEWG）和政府专家组（GGE）的作用，支持在联合国框架下制定各方普遍接受的网络空间负责任国家行为规则、准则和原则。

12.完善共享共治的国际治理机制。支持联合国互联网治理论坛（IGF）、世界互联网大会（WIC）、世界移动大会（MWC）、国际电信联盟（ITU）等平台发挥积极作用，推动政府、国际组织、互联网企业、技术社群、社会组织、公民个人，共同参与网络空间国际治理。

13.平等参与互联网基础资源管理。保障各国使用互联网基础资源的可用性和可靠性，推动国际社会共同管理和公平分配互联网基础资源。

14.推动对新技术新应用的有效治理。积极利用法律法规和标准规则引导人工智能、物联网、下一代通信网络等新技术新应用，推动在技术标准、伦理准则方面开展国际合作。

15.推动网络空间治理能力建设。搭建多渠道的交流平台，在联合国等多边框架下增设网络空间国际治理援助和培训项目，帮助广大有需求的发展中国家提升参与国际治理的能力。

成果共同分享

坚持以人为本、科技向善，缩小数字鸿沟，实现共同繁荣。

16.共享电子商务发展红利。畅通贸易渠道，减少市场准入壁垒和其他壁垒。促进跨境电子商务发展，探索建立信息共享和互信互认机制，鼓励使用安全可靠的数字化手段促进跨境贸易便利化。

17.让中小微企业更多从数字经济发展中分享机遇。鼓励各国加大政策支持，帮助中小微企业利用新一代信息技术促进产品、服务、流程、组织和商业模式的创新，增加就业机会，

积极融入全球价值链。

18.加强对弱势群体的支持和帮助，不让一个人掉队。推动互联网助力精准扶贫的经验交流与分享，促进国际减贫合作。鼓励开发适合老年人、残疾人、妇女、儿童使用的产品和服务，采取多种政策措施和技术手段，提高弱势群体的数字技能，促进公众数字素养的普及和提升。

19.加强网络文化交流与文明互鉴。尊重网络文化的多样性，提倡各国挖掘自身优秀的文化资源开展网络交流合作和文明互鉴。搭建包容、开放、多样的网络文化交流平台与机制。

20.为落实联合国 2030 可持续发展议程做出积极贡献。呼吁各国重视发展中国家关切，弥合数字鸿沟，通过信息通信技术促进持久、包容和可持续的经济增长和社会发展。

互联网是人类共同的家园，全人类从未像今天这样在网络空间休戚与共、命运相连。维护一个和平、安全、开放、合作、有序的网络空间，就是在维护我们自己美好的家园。展望前路，我们愿同国际社会一道，把握机遇，迎接挑战，携手构建更加紧密的网络空间命运共同体，共同开创人类更加美好的未来。（来源：世界互联网大会组委会）

➢ “人脸”算个人信息吗？

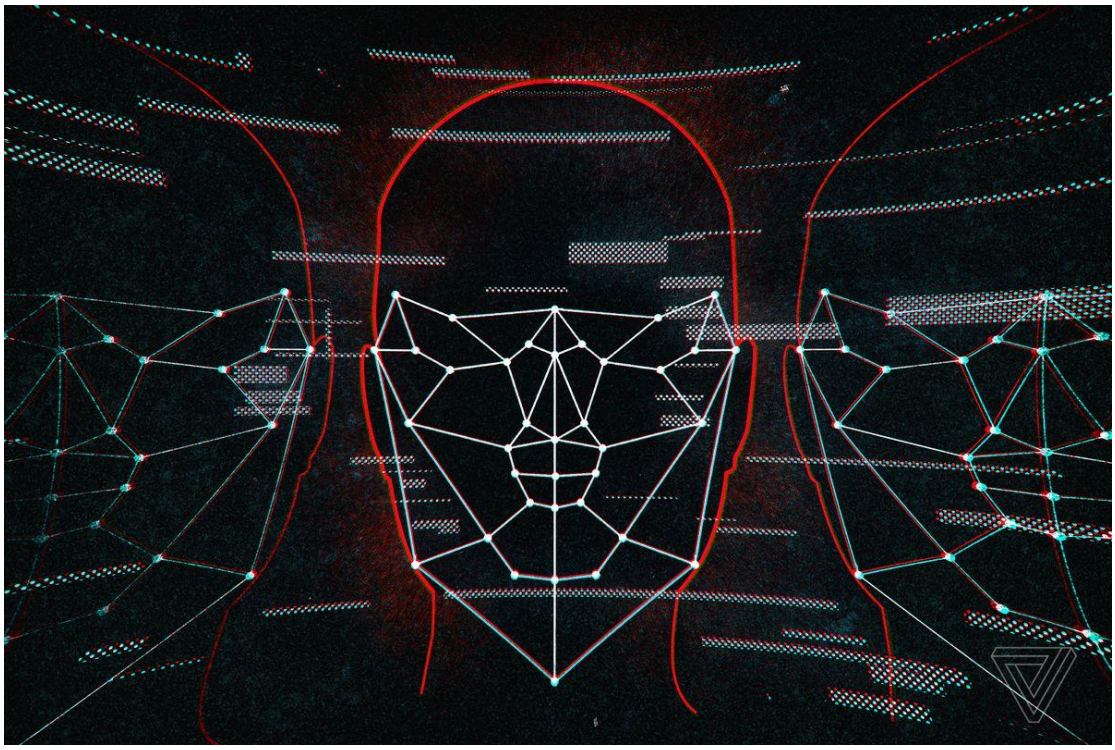
近日，《杭州市物业管理条例（修订草案）》引发网络热议，其中规定了物业服务人不得强制业主通过指纹、人脸识别等生物信息方式使用共用设施设备，保障业主对共用设施设备的正常使用权。随着智慧社区建设的推进，越来越多的小区开始安装人脸识别门禁，点赞者称人脸识别方便小区安保管理，拍砖者则认为随意采集个人信息程序违法，甚至担心数据信息泄漏造成不良后果。众说纷纭的背后，是对收集个人信息的合理性与合法性的讨论。

那么，“人脸”是否属于个人信息？法律对于“收集”行为是如何规定的？人脸识别进社区的正确方式是什么？

个人敏感信息包括“人脸”

人脸识别是基于人的面部特征进行身份识别的一项生物识别技术，这项技术通过采集人像、关键点提取，对人像进行预处理、特征提取、人脸识别对比，实现个人身份识别验证的目的。人脸识别技术始于 20 世纪 60 年代，随着大数据、互联网时代的到来，目前广泛应用于安保、移动支付、公司管理等领域。各地多个社区推广人脸识别，正是在安保、物业管理场景下的应用。

即将实施的民法典详细明确了个人信息的具体内容。个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。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。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。



2020 年 10 月 1 日实施的《信息安全技术个人信息安全规范》，进一步区分了一般个人信息和个人敏感信息。个人敏感信息指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息，具体可包括身份证件号码、个人生物识别信息、银行账户、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14 岁以下（含）儿童的个人信息等。个人信息控制者通过个人信息或其他信息加工处理后形成的信息，如一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的，也属于个人敏感信息。

因此，将“人脸”界定为个人敏感信息是合理的。个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开等，社区推广人脸识别引发争议的焦点集中于信息的收集行为。

“人脸”采集的合法性与合理性

上述《杭州市物业管理条例（修订草案）》中所规定的“物业服务人不得强制业主通过

指纹、人脸识别等生物信息方式使用共用设施设备，保障业主对共用设施设备的正常使用权”，属于新增条款，多家媒体将其解读为全国首部将小区人脸识别纳入物业管理的法定条例，与全国其他省市“来势汹汹”的人脸识别潮形成明显对比。

物业服务合同双方权利义务受合同法的约束，合同法并没有对“收集个人信息”的行为进行规定，且民法典也没有明确“收集行为”的具体含义，所以杭州市将物业服务人收集业主个人信息的行为纳入条例内容难能可贵。

《信息安全技术个人信息安全规范》对个人信息的收集行为进行了明确。收集是获得个人信息的控制权的行为，包括由个人信息主体主动提供、通过与个人信息主体交互或记录个人信息主体行为等自动采集行为，以及通过共享、转让、搜集公开信息等间接获取个人信息等行为。如果产品或服务的提供者提供工具供个人信息主体使用，提供者不对个人信息进行访问的，则不属于本规范所称的收集。例如，离线导航软件在终端获取个人信息主体位置信息后，如果不回传至软件提供者，不属于个人信息主体位置信息的收集。

民法典将收集行为列为处理个人信息的一种，应当遵循合法、正当、必要原则，不得过度处理，并遵循四个条件：一是征得该自然人或者其监护人同意；二是公开处理信息的规则；三是明示处理信息的目的、方式和范围；四是不违反法律、行政法规的规定和双方的约定。有规则，就有例外。处理个人信息免除民事责任的三个例外条件是：一是在该自然人或者其监护人同意的范围内合理实施的行为；二是合理处理该自然人自行公开的或者其他已经合法公开的信息，但是该自然人明确拒绝或者处理该信息侵害其重大利益的除外；三是为维护公共利益或者该自然人合法权益，合理实施的其他行为。

因此，对于人脸识别进社区，其合法性是在个人信息保护的多层法律框架内讨论，即是否符合民法典及《信息安全技术个人信息安全规范》等相关法律的规定。例如不应以欺诈、诱骗、误导的方式收集个人信息；不应隐瞒产品或服务所具有的收集个人信息的功能；不应从非法渠道获取个人信息。今年10月首次亮相的《个人信息保护法（草案）》中，规定了个人在个人信息处理活动中的权利，即个人对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理。

而人脸识别进社区的合理性，是在法律上常用的比例原则内进行讨论，即生活日常的场景下是否有必要收集、利用个人敏感信息。我们应当坚持收集个人信息的最小必要原则，一方面收集的个人信息的类型应与实现产品或服务的业务功能有直接关联，直接关联是指没有上述个人信息的参与，产品或服务的功能无法实现；另一方面，自动采集个人信息的频率应是实现产品或服务的业务功能所必需的最低频率。再者，间接获取个人信息的数量应是实现

产品或服务的业务功能所必需的最少数量。

强制人脸识别或引发诉讼

《杭州市物业管理条例（修订草案）》禁止物业强制人脸识别条款的建议者为浙江理工大学特聘副教授郭兵，他作为“中国人脸识别第一案”的原告，曾将杭州野生动物世界诉至法院。

2019年4月，郭兵在杭州野生动物世界办理了一张1360元的双人年卡。为了方便公园进行身份核验、防止他人冒用年卡，郭兵在办卡时录入了姓名、手机号、指纹等信息。办理年卡后，他一直使用“年卡+指纹”的方式入园。3个月之后，杭州野生动物世界先后两次发短信通知称，园区系统升级，指纹识别将取消，年卡用户不注册人脸识别将无法入园。郭兵不愿意被强制刷脸，不同意动物世界强制人脸识别的要求。杭州野生动物世界表示，如果郭兵退卡，则需要按照正常入园价格，补齐办理年卡以来数次入园的费用。

郭兵不同意这一解决方案，将杭州野生动物世界诉至法院，认为面部特征等个人生物识别信息属于个人敏感信息，一旦泄露、非法提供或者滥用极易危害消费者的人身和财产安全。郭兵要求确认杭州野生动物世界店堂告示和短信通知内容无效，退还年卡卡费，赔偿交通费并删除其个人信息。杭州野生动物世界辩称，是在征得郭兵同意的情况下收集个人信息的，双方订立的服务合同合法有效。

目前并未检索到上述案件的审理结果，而且中国人脸识别第一案是在合同法框架内进行审理，争议焦点为单方变更合同履行内容是否构成违约的问题，并非民法典意义中的非法收集行为对人格权的侵犯。

从上述案件来看，未经权利人同意强制收集“人脸”信息可引发诉讼，因此在个人信息的处理中，征得权利人同意是十分重要的。另外，我们也曾从媒体报道中看到在明星演唱会上利用人脸识别技术抓到逃犯的新闻，很少有人会对此提出异议，因此可以说，技术利用的目的是判断技术利用合理性、正当性的重要标准，而技术利用的法律依据则是判断合法性的重要标准。

人脸识别进社区的正确方式

大规模推行人脸识别进社区，方式不当或将引发法律纠纷。因此，人脸识别进社区也需要先合规。那么，什么是人脸识别进小区的正确方式呢？

首先，业主知情同意是前提。依据《信息安全技术个人信息安全规范》的要求，收集个人敏感信息前，一方面，应征得个人信息主体的明示同意，并应确保个人信息主体的明示同意是其在完全知情的基础上自主给出的、具体的、清晰明确的意愿表示；另一方面，应单独

向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得个人信息主体的明示同意。

其次，给予业主充分的决定权。无论采用何种方式进行社区建设，其目的都是为业主营造舒心、温暖的居住环境，社区管理只是营造居住环境的手段而不能作为目的。人脸识别进小区的同时，要为有异议的业主提供其他身份核验的选项，例如 NFC 卡、出入证、手动登记等多元化的选择。

最后，明确人脸识别的责任主体。民法典明确了个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开等，任何一个环节出现问题，都将导致数据泄漏，将权利人置于未知风险之下。现有的人脸识别进社区活动牵头者众多，招标标准不同，对外宣称的数据保管方式也千差万别，因此需要加快立法明确责任主体。在法律保护框架不完善的现实情况下，是否可以参照产品质量责任中销售者与生产者连带责任的方式，确定所有环节责任主体连带责任，以提高上游收集者对于下游进一步处理者的选择门槛，提高数据安全性。

（来源：北京日报）

➢ 关于我国数据治理法治构建的几点思考

一、从网络治理到数据治理

数据治理是网络治理的衍生命题，甚至已经是或者将成为替代性命题。从传统社会管理到网络社会治理，对共性问题的发现与规制是网络法治的基本路径。网络治理所要解决的问题，是网络与有关行业、业态融合的过程中，将自身的问题复制到融合的新行业、新业态所产生的。这些问题，是网络所特有的，与之相融合的行业、业态所不具有的，会随着融合的过程，成为新业态所不得不面对的问题。网络治理所要解决的就是由于网络融合所出现的共性问题。数据治理是共性问题中的共性问题，在当前阶段具有格外重要的地位。数字经济已经成为经济发展的新动能，数据的潜力正在不断凸显，同时也产生了一系列的问题。过去的共性问题不断数据化，新型的数据问题不断产生。网络安全问题聚化为数据安全问题，比如跨境数据流动、数据泄露等问题。个人信息问题与个人数据问题本质上相互等同，受到广泛地关注。网络信息服务管理在很大程度上是对数据的控制问题，表现为政企之间数据配合程度或者配合义务的问题。与此同时，数据垄断、数据滥用、数据权属、数据流通等新型问题也大幅进入研究和管理视野。网络治理的问题已经阶段性地演变成数据治理的问题，而这一

阶段可能会持续相当长的时间。关于“数据”，有很多种认识，将之比拟为 21 世纪的“石油”和“黄金”。这种重要性的认识还比较粗放，也符合数字经济仍处于发展前期的客观实践。随着数字经济的持续深入发展，对数据的认识还会进一步深入化、精细化。当前阶段围绕数据所产生的一些问题、矛盾，将依赖于更深层次的理解和认识而得以妥善解决。

数据的问题可以大致划分为三个领域，数据价值、数据安全和用户保护。数据价值属于目标性问题，也就是数据治理的最终目标，一般有赖于促进性的政策予以保障，但是也包括数据权属等基础性问题需要立法明确。数据治理的法治体系就是按照数据价值、数据安全和用户保护三个方面推进的。总体上来看，三者之间需要取得平衡的关系。这种平衡关系并不能简单地得出结论，而是至少应该用“成本-收益”分析的基本方法来进行制度设计。因为，三者之间零和博弈十分明显，处于此消彼长的相互关系。不难理解，对数据安全的要求更为严格，就会限制数据价值释放的空间。数字化社会的快速来临，加快了数字红利的稀释速度，同时也促使了数字恐慌的加剧蔓延。针对数据安全的认识多以感性为基础，而缺乏具体的理论支撑和实证研究。从法社会学的角度来看，当前阶段对数据安全的推崇在一定程度上也是对社会情感的安抚。我们知道，网络具有开放性和交互性，很难实现绝对安全，只能不断获得相对安全。数据安全立法过程中需要认识并坚持这一点。按照法经济学的思路，围绕数据安全（包括用户保护）的法律制度构建，需要进行成本分配的精确测算。

二、数据价值问题

党中央连续多次就数据价值释放的问题发布重要文件。2019 年 11 月，党的十九届四中全会在《中共中央关于坚持和完善中国特色社会主义制度 推进国家治理体系和治理能力现代化若干重大问题的决定》中首次明确数据作为生产要素参与社会分配。2020 年 3 月发布的《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》中提出，要加快培育数据要素市场，推进政府数据开放共享，提升社会数据资源价值，加强数据资源整合和安全保护。2020 年 5 月发布的《中共中央 国务院关于新时代加快完善社会主义市场经济体制的意见》中提出，要加快培育发展数据要素市场，建立数据资源清单管理机制，完善数据权属界定、开放共享、交易流通等标准和措施，发挥社会数据资源价值。推进数字政府建设，加强数据有序共享，依法保护个人信息。

促进性措施由政策调整更为合适，但是立法的作用也很重要，以回应一些基础性问题，比如数据权属。目前数据权属在法律层面没有定论，给数据流通、数据交易带来障碍。现行《网络安全法》《刑法》（修正案九）侧重于保护公民个人信息的角度，规定较为严格，个人信息交易流通的合法空间十分有限。欧盟《数据战略》中指出，数据的价值在于能够使用和重用。能够重用的前提是数据能够被更广泛地共享，而只有自由、灵活的交易流通机制才能保证数据共享的广泛性，最大程度激活数据的价值。按照传统经验和实践效果，只有对数据予以较为充分的确权，数据交易流通才能得到保障。

不过，最为寄予厚望的《民法典》在一定程度上回避了这一问题。2020 年 5 月 28 日颁布的《民法典》延续了《民法总则》的思路，对个人信息采取了权益保护而非权利保护的安排。这对于法理来说，无疑产生了一些遗憾和争议。但是对于数据实践，却留出了相对灵活的空间。采用权益保护的思路，一方面能够保证用户权益保护的法律依据，另一方面又避免了强权利保护可能对数据产业造成过于强硬的影响。不过这无疑也是一种稳妥处理的法律思路，体现了法律客观反映实践规律的谨慎性，避免过早给出极端的法律结论。

相比之下，地方立法更具探索性，试图取得区域性立法突破。2020 年 7 月，深圳市发布《深圳经济特区数据条例（征求意见稿）》，创设性规定了“数据权”的概念，针对不同的数据类型明确数据权归属。自然人对其个人数据依法享有数据权；公共数据属于新型国有资产，数据权归国家所有；数据要素市场主体对其合法收集的数据和自身生成的数据享有数据权。不过，条例没有对不同主体数据权发生冲突采用何种解决原则或规则并未进行规定。同月，天津市发布了《天津市数据交易管理暂行办法（征求意见稿）》对数据交易双方的数据权进行了规定，要求交易数据必须无权利争议，经处理无法识别特定数据提供者且不能复原，数据需方不得对数据进行重新识别，按约定完成使用后应及时销毁数据。地方立法在多大程

度上能实现对基本民事权利义务关系的突破，还存在一些质疑。

未来，数据权属问题始终有待解决。这是一个法律问题，同时也是经验问题或者技术问题。现在来看，数据价值释放程度还比较浅显，社会关系较为简单。实际上，数据价值的潜力可能远超出既有的想象。有学者就提出“权利束”“新型财产权利”等较为复杂的理论模型来解释数据权属可能形成的复杂关系。如何界定数据权属，在一定时间内可能还会是一个难解的命题，也很难形成各方满意的最优解，最后还是一个利益平衡、有所取舍的结果。

三、数据安全问题

相比于数据价值，数据安全是底线性问题，主要是解决数据价值释放中可能产生的风险和负面效果，这些需要通过法治建设来加以保障。其中，用户保护也就是个人信息保护的问题，广义上可以归入数据安全问题（如《网络安全法》就将“个人信息保护”放入“网络信息安全”一章），但是近些年来，个人信息保护问题十分重要也广为关注，因此也可以从数据安全中剥离出来，与之相并列。不过，用户保护与数据安全一样，都侧重于风险规制。

数据安全问题在《网络安全法》中有所规定，主要是对关键信息基础设施的数据安全进行了规定，最为核心的是第三十七条有关数据跨境的要求。围绕这一条的讨论十分激烈，国家互联网信息办公室也相继发布了个人信息、重要数据出境安全评估管理办法的征求意见稿。目前数据安全问题还没有专门的立法，国外立法经验也比较少见。比较重要的两部立法仍然处于制定阶段，一部是《数据安全管理办法》，另一部是《数据安全法》。

《数据安全管理办法》2019 年 5 月由国家互联网信息办公室向社会公开征求意见，规范中华人民共和国境内利用网络开展数据收集、存储、传输、使用等活动，对数据安全进行全生命周期管理，主要是确立数据分级分类管理以及风险评估，检测预警和应急处置等管理制度。《数据安全管理办法》中的很多制度与欧盟 GDPR 的规制思路有些类似，比如日常安全保障、风险评估等，填补了国内数据安全管理的一些制度空白。其中，争议比较大的是主体问题，有观点认为《数据安全管理办法》对于《网络安全法》有所突破，将数据安全的部分责任由“关键信息基础设施运营者”扩大为“网络运营者”，使得本不在《网络安全法》调整范围的一部分主体也将承担相应的义务。对此，实际的数据安全管理需求与法律制度的相对保守形成了冲突。因此，《数据安全法》作为后法，以及与《网络安全法》同一位阶的立法，如何对数据安全问题作出制度安排，就显得尤为重要。

《数据安全法（草案）》于 2020 年 6 月提交全国人大常委会进行第一次审议。草案与《数据安全管理办法》相类似，构建了网信部门牵头、有关部门依据职责监管的体系，特别是对“各部门、各地方”予以更大空间的授权。同时，也规定了分级分类、日常保障、应急

管理等基本制度。但其内容与公众的预期尚存差距。这其中反映了对数据本身、对数字经济发展阶段、对安全与发展平衡等问题认识程度的不一致。因此，如何对数据安全进行制度设计，仍然留有较大的讨论空间。从数据利用的趋势来看，秉持“利用是原则，不利用是例外”应当是未来数据治理的主要思路。按照这一思路，制度设计就面临选择，是进行全生命周期管理，还是聚焦重点环节。搞清楚数据治理的关键问题，并有针对性的做出制度回应，可能更能反映数据活动的客观规律。

四、个人信息保护问题

国内个人信息保护立法处于分散的状态，《网络安全法》《消费者权益保护法》《电信和互联网用户个人信息保护规定》在一般层面对个人信息保护问题做出了总体性规定，金融、健康、交通、电子商务等领域对个人信息保护进行了行业性规定。国外个人信息保护统一立法趋势十分明显，特别是欧盟的 95 指令和 GDPR 对世界范围内个人信息保护立法产生了重大的影响。

目前主流个人信息保护立法主要包括三个方面的内容：一是个人信息保护专门机构。从欧盟实践来看，个人信息保护机构在个人信息保护中发挥了重要的作用，有效地适应了个人信息保护动态性、区分性的特点。强有力的个人信息保护机构能够根据具体问题、具体领域和具体时点做出相应的判断和解释，以弥补立法机械、保守的固有特点。二是个人享有的权利。这是个人信息保护的主要内容。GDPR 列举了较为全面的个人信息权利，包括知情权、访问权、删除权（被遗忘权）、更正权、可携带权等。不同国家根据不同国情可以做出不同的选择，权利配置一方面决定了对个人的保护水平，另一方面也框定了数据产业的发展空间。三是监管制度。主要包括数据保护官（数据登记注册）、日常安全保障、风险评估、泄露通知、应急处置等方面。这些制度在各国个人信息保护立法和实践中大同小异，关键在于以何种标准、指引的方式予以支撑，确保其具备操作性，发挥实际的作用。

2020 年 10 月 14 日，我国刚刚第一次审议了《个人信息保护法（草案）》。其中对个人信息保护的主体内容进行了回应：一是以《民法典》为基础明确个人信息保护的具体权益，包括知情权、查询复制权、删除权等，同时进一步增加了解释权、决定权、限制处理权等（根据前述，此处应该理解为权益而非权利）。二是充分反映实际运转的管理机制并进行制度性固化。《个人信息保护法（草案）》突出了网信部门统筹协调的作用，也明确了各有关部门依据职责进行分工。三是明确日常和应急保障制度，个人信息处理者应当制定内部管理制度和操作规程，采取相应的安全技术措施，定期对其个人信息活动进行合规审计。同时还建立了数据保护专员、高风险评估等制度，并且进一步明确了数据泄露通知制度的具体要求。（作

者：中国信息通信研究院互联网法律研究中心主任　方禹）

➢ 网络安全即服务的业务前景分析

一、当前网络安全服务存在本末倒置情况

网络安全服务，一直是让国内网络安全公司纠结的业务。自 2016 年国内开展网络安全实网攻防演习以来，每年演习期间安全服务人员的服务费一路走高，还在网络安全培训班学习的学生就可以达到每天几千元的水准，高水平安服人员的服务费甚至能达到每天数万元。但当演习结束后，网络安全服务依然是“不能没有，但不挣钱”的局面。网络安全公司深知安全服务的重要性，但面对安服人员薪酬日益升高、流动性越来越大、依然疲软的客户买单意愿等问题，依然难以下决心扩大安服团队规模。

中国网络安全产业的一大痛点是用户愿意为硬件出高价，而不愿意在软件上多花钱，对于服务更是要求免费。实际上随着半导体技术的进步，硬件在网络安全产品中的价值逐渐降低，即使防火墙这种需要进行大流量处理的设备，采用通用芯片后电路部分所完成的功能也是高度同质化的，运行在硬件电路之上的软件才是完成安全设备主要功能的功臣。而要把安全设备真正使用起来，实现有效的防御，则需要掌握网络安全知识、理解用户需求、懂得攻防技术的网络安全工程师。

这种价值观上的本末倒置，导致市场上劣币驱逐良币现象的发生：安全服务只是证明用户现有系统存在安全问题的“敲门砖”，成为网络安全公司软硬件产品销售的“添头”。因为

安全服务本身难以为公司带来大的销售额和利润，在有的公司甚至被当作“成本中心”。在过去很长一段时间，即使是国内头部的网络安全公司，也只维持一百来人的安服团队规模，难以为众多的客户提供所需的安全服务。

网络安全服务的内容很广泛，但在国内的发展很不均衡。渗透测试服务因为能直接帮用户发现系统中的安全问题，从而促成销售，被广泛接受；测评类服务因为是 ISO27000 认证、等级保护测评等合规性要求的必选项，也有稳定的市场；但安全顾问咨询类服务在国内的发展较差，相关公司营收很低；MSSP、MDR 等安全托管类业务目前还是边缘化业务。

二、网络安全服务的市场发展前景

上述问题的成因不管是商业文化、招投标制度，还是价值度量问题，之前已经有很多分析，在这里不再展开赘述，我们更需要关心的是如何改变现状。

首先看存量市场，谁在购买网络安全服务？在过去的 20 多年，网络安全服务的买单者主要是网络安全市场的头部客户：政府、金融、电信运营商、大型国企、大型商业企业。这些客户共同的特点是，所从事的业务重要性高，营收规模大，IT 预算相对充裕，往往会有自己专门的网络安全团队，对供应商相对强势，采购网络安全服务是为了弥补自身网络安全团队能力的不足或解决人手不够的问题。

近两年由于安全事件频发以及实网演习的影响，部分头部客户开始意识到安全服务的重要性，增加在安全服务上的预算，用采购安全服务的方式代替网络安全软硬件产品的采购，将买来的网络安全设备真正用起来。但由于受管理体制的制约和预算模型、招投标制度的限制，以及领导对网络安全认知局限性等问题，网络安全服务市场想出现大的改变还需要时间。

远水难解近渴，我们还要看增量市场有哪些。我们正处在整个社会快速数字化转型的历史时期，在经历了消费互联网快速发展的 20 年之后，5G、物联网、大数据、人工智能驱动的产业互联网，正在更深刻地改变着社会的运行方式。所谓“数字经济”，是指人类通过对数字化的知识与信息的识别、选择、过滤、存储、使用，引导、实现资源的快速优化配置与再生，实现经济高质量发展的经济形态。对企业来说，是通过资源优化配置，提高生产效率，降低生产成本，为用户提供个性化的产品或服务，在商业竞争中获得竞争优势。在工人的人力成本逐渐走高以及更加难以管理的情况下，采用工业互联网技术的工厂能用更少的人力消耗、更低的综合生产成本，更快地为用户提供个性化的产品，这已经成为富士康等大型制造企业的选择。而便利蜂等新型便利店，通过信息化、网络化手段，实现一个店长就可以维持一个便利店的正常运行，也是通过技术手段来降低运营成本。

但是，数字经济在让企业获得竞争优势的同时，也让企业有更多的攻击面暴露在互联网

上，网络攻击可能带来的生产停顿、与客户失联、用户数据泄露等后果，会让企业面临经济损失或遭到主管机构处罚乃至吊销经营许可的风险，迫使企业不得不在网络安全方面加大投入，尽可能保证业务的正常开展，这时企业会遇到安全能力供应与成本两个问题。

作为企业，一定要计算 ROI（投资回报率），网络攻击的发生以及造成的后果都具有一定的发生概率。而网络安全方面的投资，不管是雇佣网络安全专家、购买网络安全产品、购买网络安全服务，都要计入经营成本，如果在网络安全上的投入抵消了数字化转型带来的好处，那么企业进行数字化转型的动力就不会很强。

大型企业因为其营业规模大，盈利能力强，雇佣几十人甚至数百人的网络安全团队，购买或自研大量的网络安全系统，针对自己的业务特点来组织网络安全防线，从投资回报率上是合算的。

但对广大的中小企业，这种自备安全团队的模式完全不适用。有数据显示，中国的中小企业数量超过 3000 万家，这些企业也在数字化转型中，用自备网络安全团队的方式进行防御，企业既无法承担网络安全防御的成本，我们也培养不出那么多的网络安全工程师。解决广大中小企业网络安全问题的出路，就在于网络安全即服务这种商业模式。

三、网络安全即服务是未来产业发展方向

网络安全即服务是在 SaaS（软件即服务）的启发下提出的一种商业模型，CSA 列出了一个网络安全即服务的目录：业务连续性与灾难恢复、持续监测、数据防泄露、电子邮件安全、加密、身份与访问管理、入侵管理、网络安全、安全评估、SIEM、漏洞扫描、网站安全，基本覆盖了企业日常安全运营的内容。

2018 年初，谷歌的母公司 Alphabet 宣布成立一家名叫 Chronicle 的网络安全公司，利用谷歌庞大的基础设施和数据分析能力，Chronicle 在 2019 年发布了一个名为 Backstory 的信息安全数据平台。我在 RSAC 2019 上，向 Chronicle 的工作人员询问了其 Backstory 的工作模式以及服务价格：服务费按企业员工数收取，每个员工每年 45 美金；不管企业有多少设备；不管企业产生了多少日志/告警；不限量分析/查询；现在还不支持的日志格式，承诺三周内就能支持。

Chronicle 用了“Telemetry（遥感勘测）”这个词来描述 Backstory 提供的服务，其工作模式是企业把各种日志上传给 Chronicle，Chronicle 帮助企业进行分析，企业的安全运维人员在 Backstory 的平台上进行查询。

显然，这是《创新者的窘境》中克里斯坦森教授所讲述的“低端逆袭”的打法，对拥有成规模的安全团队、安全预算也不是大问题的“高端客户”来讲，Chronicle 的服务吸引力并

不大，但对无法负担专业的安全团队、安全预算有限的中小企业来讲，Backstory 是很有吸引力的服务。并且如果 Backstory 确实好用，那么它会逐步向上蚕食中高端用户市场。

此外，作为 Alphabet 旗下公司，如果能充分整合利用谷歌的资源，Backstory 就能做到既便宜又好用：谷歌拥有 Virus Total，这是全球最大的恶意样本库，解决了样本与 URL 威胁情报的来源问题；谷歌拥有 8.8.8.8 的 DNS，全球约有 13%的域名解析是由谷歌提供，DNS 解析信息是一个非常宝贵的威胁情报来源，并且可以通过 DNS 解析进行部分防护服务工作；谷歌拥有搜索引擎，对通过网页进行传播的恶意代码有很强的追溯能力；谷歌拥有 Chrome 浏览器，能从浏览器的行为日志/异常告警发现网络攻击；谷歌拥有先进的分布式存储、分布式计算平台，可以用极低的成本实现海量数据的存储与检索；谷歌拥有先进的人工智能技术与自然语言处理技术，对日志文件的分析很大程度上可以通过自动化手段进行；谷歌 Project Zero （GP0）团队的漏洞挖掘能力全球领先。

有效整合了谷歌以上各威胁情报和网络安全能力，Chronicle 就能通过资源复用而大幅降低安全服务的边际成本。果不其然，2019 年 6 月，即传出 Chronicle 被整合进谷歌 Cloud 业务的消息。虽然在 2019 年 11 月份时，Chronicle 曾被媒体报道一系列负面消息，例如人员流失/转岗等，但我觉得断言 Chronicle 的失败还为时过早，企业级的网络安全业务演进速度慢，云化的、低成本、高服务带宽的网络安全服务，是解决网络空间安全问题的出路之一，是未来的大方向。

四、我国网络安全即服务的发展分析

国内的网络安全即服务业务还处于发展的初级阶段，未来可能会有三种类型的公司开展

这项业务。

大型云服务商：阿里云、腾讯云等已经为使用其云服务的企业提供了与云服务相关的网络安全防御服务，阿里云 2019 年的云安全服务收入已经相当于一家大型综合网络安全公司的全年营收。安全是云服务客户的刚性需求，云服务商为了自身云服务的安全会配备实力很强的网络安全团队。网络安全即服务未来会是云平台提供的服务之一。

电信运营商：在 Gartner 的 MSSP（网络安全托管服务提供商）魔力象限中，AT&T、Century Link、Verizon、NTT 都是头部厂商。中国电信与中国联通分别推出了云堤与云盾抗 DDos 服务。此外，中国电信与中国联通在 MSS（安全托管服务）业务上也都做过一些尝试，中国电信推出的“安全管家”服务，部分省份与安全公司合作提供 MSS/MDR 服务给线路租用客户，合作的安全公司一个月能拿到数百万人民币的收入分成，虽然业务规模尚不大，但也是很有意义的探索。电信运营商依靠其在网络链路、威胁情报、触达客户的能力上的优势，具备更低成本提供网络安全服务的条件，其短板是网络安全能力，与网络安全公司合作提供安全服务是一个达成双赢的方法。并且电信运营商在国家的网络安全防线中肩负着无可替代的责任，发展网络安全能力是必然选择。

网络安全公司：优势是具备专业安全服务人员，有服务经验。但业务模式的变化意味着公司要走出之前的舒适区，面临的挑战也不小。与云服务商以及电信运营商相比，传统网络安全公司在网络安全即服务业务上批量获客能力以及规模经营上会有劣势。

网络安全即服务业务在中国的健康发展还需要两个突破：

首先，是对远程服务的政策许可。用户习惯了“物理隔离”“逻辑隔离”的网络管理方法，首先会怀疑远程服务的安全性。这个问题可以通过技术与法律双重手段解决，技术的进步已经使得我们有能力对远程安全运维人员做多维度的监控和审计，新冠疫情期间很多工作如考试都可以远程进行。远程运维令牌、生物识别、操作审计、网络审计、行为审计、摄像头监控都是可以采用的技术手段。

其次，要解决网络安全产品的接口标准化与 SIEM、SOC、SOAR 系统的工作效率与有效性。生产效率的提高需要自动化、半自动化工具与网络安全产品、网络安全服务人员的高效协同，目前国内网络安全产品的接口标准化程度要差一些，对 SIEM、SOC、SOAR 系统的技术挑战会更大。

一个服务对客户的价值决定企业的价值，网络安全即服务用相对较低的成本就能保障生产、生活的相对安全，这个领域未来将会产生很高商业价值的企业。（来源：《中国信息安全》杂志 2020 年第 10 期）

四、政府之声

➢ 《互联网直播营销信息内容服务管理规定（征求意见稿）》公开征求意见

2020 年 11 月 13 日，国家互联网信息办公室日前对外发布《互联网直播营销信息内容服务管理规定（征求意见稿）》（以下简称《征求意见稿》），对直播营销平台、直播间运营者和直播营销人员等作出具体规范。

《征求意见稿》明确，互联网直播营销信息内容服务是指通过互联网站、应用程序、小程序等，以视频直播、音频直播等形式向社会公众推销商品或服务的活动。

《征求意见稿》明确，直播营销平台应当建立健全账号及直播营销业务注册注销、信息安全管理、营销行为规范、未成年人保护、用户权益保护、个人信息保护、信用评价、数据安全等机制。

《征求意见稿》要求，直播营销平台加强互联网直播营销信息内容服务管理，发现违法和不良信息，应当立即采取处置措施，保存有关记录，并向有关主管部门报告。直播营销平台应当防范和制止违法广告、价格欺诈等侵害用户权益的行为，以显著方式警示用户平台外私下交易等行为的风险。应当根据直播间运营者账号信用评价、关注和点击数量、营销金额及其他指标维度，建立分级管理制度，对重点直播间运营者采取安排专人实时巡查、延长直播内容保存时间等措施。应当建立健全风险识别模型，对高风险行为采取弹窗提示、违规警告、限制流量、阻断直播等措施。应当建立黑名单制度，将严重违法违规的直播营销人员及因违法犯罪或破坏公序良俗造成恶劣社会影响的人员列入黑名单。

《征求意见稿》还对直播营销人员或者直播间运营者作出规范，明确直播间运营者、直播营销人员从事互联网直播营销信息内容服务，应当真实、准确、全面地发布商品或服务信息，不得从事的行为包括：发布虚假信息，欺骗、误导用户；虚构或者篡改关注度、浏览量、点赞量、交易量等数据流量造假；知道或应当知道他人存在违法违规或高风险行为，仍为其推广、引流；侮辱、诽谤、骚扰、诋毁、谩骂及恐吓他人，侵害他人合法权益；可能引发未成年人模仿不安全行为和违反社会公德行为、诱导未成年人不良嗜好等；涉嫌传销、诈骗、赌博、贩卖违禁品及管制物品等。（来源：中国网信网）

- **《互联网直播营销信息内容服务管理规定（征求意见稿）》**
- **全文：**http://www.cac.gov.cn/2020-11/13/c_1606832591123790.htm

➢ 国家市场监管总局发布《关于平台经济领域的反垄断指南（征求意见稿）》

2020 年 11 月 10 日，国家市场监督管理总局发布《关于平台经济领域的反垄断指南（征求意见稿）》（以下简称征求意见稿），其中平台“二选一”、大数据杀熟、低价倾销成为重点监管领域。此前数日，市场监管总局、中央网信办、税务总局三部门联合召开规范线上经济秩序行政指导会，《经营者集中审查暂行规定》《规范促销行为暂行规定》《关于加强网络直播营销活动监管的指导意见》相继出台。

此次征求意见稿共 24 条，明确了对平台经济领域开展反垄断监管要坚持营造公平竞争

秩序、加强科学有效监管、激发创新创造活力、促进行业健康发展和维护各方合法利益的原则。

中国人民大学法学院教授刘俊海表示：随着平台经济发展日渐成熟，不少平台企业逐渐从规模快速扩张期转入资源掌控期，不规范竞争行为集中出现。征求意见稿将进一步推进企业竞争公平化、市场治理现代化、市场环境法治化。对于引起广泛争议的平台“二选一”问题，征求意见稿作出专门规定，并规定了认定是否构成限定交易重点考虑的两种情形，一是当平台经营者通过惩罚性措施实施限制从而产生直接损害时，一般可认定构成限定交易行为。二是当平台经营者通过激励性方式实施限制，虽然可能会具有一定的积极效果，但如果具有明显的排除、限制竞争影响，也将被认定为限定交易行为。

刘俊海表示，征求意见稿对“二选一”行为作出规定，弘扬了公平与效率并举更加注重公平的精神，符合广大消费者的最佳利益，符合互联网行业公平竞争的需要，下一步要将重点放在政策落地见实效上。对于大数据杀熟问题，征求意见稿表示，具有市场支配地位的平台经济领域经营者，可能会基于大数据和算法，对新老交易相对人实行差异性交易价格或者其他交易条件。不过，征求意见稿也规定，如果平台经营者是针对新用户的首次交易在合理期限内开展的优惠活动，则可以不被认定为差别待遇行为。

此外，征求意见稿也将涉及协议控制（VIE）架构的经营者集中纳入经营者集中反垄断审查的范围。同时对平台经济领域内的滥用行政权力排除、限制竞争行为作出了规定，并要求行政机关制定涉及平台经济领域市场主体活动的规章等时，应当进行公平竞争审查。据悉，市场监管总局接下来还将制定出台《网络交易监督管理办法》等一批规范线上经济发展的制度措施。（来源：国家市场监督管理总局）

- **《关于平台经济领域的反垄断指南（征求意见稿）》**
- **全文：**http://www.samr.gov.cn/hd/zjdc/202011/t20201109_323234.html

➢ 工业和信息化部发布关于下架侵害用户权益 APP 的通报

2020 年 11 月 10 日，工信部发布通报称，将组织下架此前未按要求完成整改的 60 款 App，包括扫描宝（版本 4.6.8）、花友（版本 4.3.10）等。

据了解，10 月 26 日，工信部曾通报了 2020 年第五批存在侵害用户权益行为的 App 名单，并强调涉及到的 131 款 App 应在 11 月 2 日前完成整改。截至目前，经第三方检测机构

核查复检，尚有 60 款 App 未按照工信部要求完成整改。

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

访客预约 | RSS订阅
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 复工复产专题

首页 > 新闻动态 > 工信动态

关于下架侵害用户权益APP的通报

发布时间：2020-11-10 14:23 来源：信息通信管理局

2020年10月26日，工业和信息化部向社会通报了131家存在侵害用户权益行为APP企业的名单。截至目前，经第三方检测机构核查复检，尚有60款APP未按照工业和信息化部要求完成整改（名单见附件）。依据《网络安全法》和《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407号）等法律和规范性文件要求，工业和信息化部组织对上述APP进行下架。

相关应用商店应在本通报发布后，立即组织对名单中应用软件进行下架处理。后续，工业和信息化部还将对未严格落实管理主体责任的部分应用商店及移动应用分发平台，存在违规收集用户个人信息行为的SDK企业，依法严厉处置。

附件：下架的应用软件名单.doc

工业和信息化部信息通信管理局
2020年11月9日

值得注意的是，通报强调，相关应用商店应在本通报发布后，立即组织对名单中应用软件进行下架处理。

此外，工信部新闻发言人、信息通信发展司司长闻库曾在新闻发布会提到，今年工信部还将加强对常用 SDK 以及应用分发平台的监管，重点针对“App、SDK 违规处理个人用户信息”“设置障碍、频繁骚扰用户”“欺骗误导用户”“应用分发平台责任落实不到位”等四个方面 10 类问题进行集中专项整治。

工信部在此次通报中表示，后续将对未严格落实管理主体责任的部分应用商店及移动应用分发平台，存在违规收集用户个人信息行为的 SDK 企业，依法严厉处置。（来源：工业和信息化部）

➢ 网络安全态势感知技术标准化白皮书（2020 版）发布

2020 年 11 月 9 日，在全国信息安全标准化技术委员会 2020 年第二次工作组“会议周”上，《网络安全态势感知技术标准化白皮书（2020 版）》正式发布。

白皮书由公安部第三研究所联合北京天融信网络安全技术有限公司、新华三技术有限公司、中国电子技术标准化研究院、北京神州绿盟科技有限公司等 16 家企事业单位共同编制。白皮书对网络安全态势感知技术的发展历程、标准化需求与现状等进行了梳理，研究给出了网络安全态势感知的技术框架和标准架构，提出了网络安全态势感知标准化工作的建议。（来源：全国信息安全标准化技术委员会）

- **《网络安全态势感知技术标准化白皮书（2020 版）》**
- **全文：**https://www.tc260.org.cn/upload/2020-11-09/1604914831845079890.pdf

五、本期重要漏洞实例

➢ Microsoft 发布 2020 年 11 月安全更新

发布日期：2020-11-10
更新日期：2020-11-10
微软发布了 2020 年 11 月份的月度例行安全公告，修复了其多款产品存在的 112 个安全漏洞。受影响的产品包括:Windows 10 20H2 & WindowsServer v20H2(52 个)、Windows 10 2004 & WindowsServer v2004（52 个)、Windows 10 1909 & WindowsServer v1909（53 个)、Windows 8.1 & Server 2012 R2 (35 个)、Windows Server 2012 (25 个)、Internet Explorer (3 个)、Microsoft Edge (HTML based)（4 个）和 Microsoft Office（15 个)。

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-2020-17051	**Windows Network File System 远程代码执行漏洞**	严重 远程代码执行	Windows 10 Server 2016 Server 2019 Server, version 1903 Server, version 1909 Server, version 2004 Server, version 20H2 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-17087	**Windows Kernel 本地提升权限漏洞**	重要 特权提升	Windows 10 Server 2016 Server 2019 Server, version 1903 Server, version 1909 Server, version 2004 Server, version 20H2 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-17042	**Windows Print Spooler 远程代码执行漏洞**	严重 远程代码执行	Windows 10 Server 2016 Server 2019 Server, version 1903 Server, version 1909 Server, version 2004 Server, version 20H2 Windows 8.1 Server 2012 Server 2012 R2

CVE-2020-17107	**HEVC Video Extensions 远程代码执行漏洞**	严重 远程代码执行	HEVC Video Extensions
CVE-2020-17058	**Microsoft Browser 内存破坏漏洞**	严重 远程代码执行	Internet Explorer 11 Microsoft Edge(EdgeHTML-based)
CVE-2020-17064	**Microsoft Excel 远程代码执行漏洞**	重要 远程代码执行	Office 2010/2013/2016/2019 365 Apps Enterprise Excel 2010/2013/2016 Office Web Apps 2010/2013 Office Online Server
CVE-2020-17061	**Microsoft SharePoint 远程代码执行漏洞**	重要 远程代码执行	SharePoint2010 SharePoint 2013 SharePoint Ent 2016 SharePoint 2019

参考信息：

https://msrc.microsoft.com/update-guide/en-us/releaseNote/2020-Nov

➢ Cisco IOS XR -bit Preboot eXecution Environment 访问控制错误漏洞

发布日期：2020-11-11

更新日期：2020-11-11

受影响系统：

Cisco IOS XR

描述：

CVE(CAN) ID: CVE-2020-3284

Cisco IOS XR 是美国思科（Cisco）公司的一套为其网络设备开发的操作系统。

Cisco IOS XR 64-bit Preboot eXecution Environment 存在安全漏洞，攻击者可以利用该漏洞通过 Cisco IOS XR 64 位的 Preboot eXecution Environment 绕过限制，以提升其特权。。

建议：

厂商补丁：

Cisco

厂商已发布了漏洞修复程序，请及时关注更新：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-pxe-unsign-code-exec-qAa78fD2

➢ Oracle Database Server 信息泄露漏洞

发布日期：2020-10-21
更新日期：2020-11-17
受影响系统：Oracle Database Server < 20.2
描述：

CVE(CAN) ID: CVE-2020-14763
Oracle Database Server 是美国甲骨文（Oracle）公司的一套关系数据库管理系统。该数据库管理系统提供数据管理、分布式处理等功能。
Oracle Database Server 20.2 版本之前的 Oracle Application Express Quick Poll 组件存在信息泄露漏洞。攻击者可利用该漏洞使用有效用户账户权限通过 HTTP 访问网络破坏 Oracle Application Express Quick Poll，对 Oracle Application Express Quick Poll 的某些可访问数据进行未经授权更新、插入或删除访问以及对其可访问数据的子集进行未经授权读取访问。
链接：https://www.oracle.com/security-alerts/cpuoct2020.html
建议：

厂商补丁：Oracle
Oracle 已经为此发布了一个安全公告（cpuoct2020）以及相应补丁
链接：https://www.oracle.com/security-alerts/cpuoct2020.html

➢ IBM InfoSphere Information Server 信息泄露漏洞

发布日期：2020-11-13
更新日期：2020-11-18
受影响系统：IBM InfoSphere Information Server 11.7
描述：

CVE(CAN) ID: CVE-2020-4886
IBM InfoSphere Information Server 是美国 IBM 公司的一套数据整合平台。该平台可用于整合各种渠道获取的数据信息。InfoSphere Information Server 11.7 版本存在信息泄露漏洞。攻击者可利用该漏洞从浏览器历史记录中获取敏感信息。
链接：https://www.ibm.com/support/pages/node/6366715
建议：

厂商补丁：
IBM
IBM 已经为此发布了一个安全公告（6366715）以及相应补丁:
6366715：Security Bulletin: IBM InfoSphere Information Server is affected by an information disclosure vulnerability
链接：https://www.ibm.com/support/pages/node/6366715

六、本期网络安全事件

➢ 印度杂货电商 BigBasket 遭黑客攻击 2000 万用户信息被泄

2020 年 11 月 9 日，援引多家印媒报道，阿里巴巴投资的印度最大杂货电商 BigBasket 近期遭受黑客网络攻击，导致大约 2000 万用户的个人数据被泄漏。这些泄漏的信息包括用户的电子邮件地址、密码哈希值、联系方式（移动和手机）、地址、生日、住址和登录 IP 地址等等，这些信息在暗网上以 300 万卢比（约 26.8 万人民币）的价格出售。

安全公司 Cybel 在 10 月 30 日发现安全泄露事件之后已经告知了 BigBasket。并且该电子商务平台已向位于班加罗尔（Bangaluru）的网络犯罪小组（Cyber Crime Cell）投诉。该公司正在评估“索赔的违反程度和真实性”。

Cyble 表示：“在我们常规的暗网监控过程中，我们的研究团队发现 BigBasket 的数据库以超过 40000 美元的价格在暗网上出售。这些泄漏的信息包括数据库部分；表名称为‘member_member’。该 SQL 文件的大小约为 15GB，其中包含近 2000 万用户数据”。

虽然该公司在 BigBasket 的客户泄露的详细信息中提到了“密码”，但应注意，该公司使用 OTP 或通过 SMS 发送的一次性密码，每次用户登录其帐户时，该密码都会不断更改。

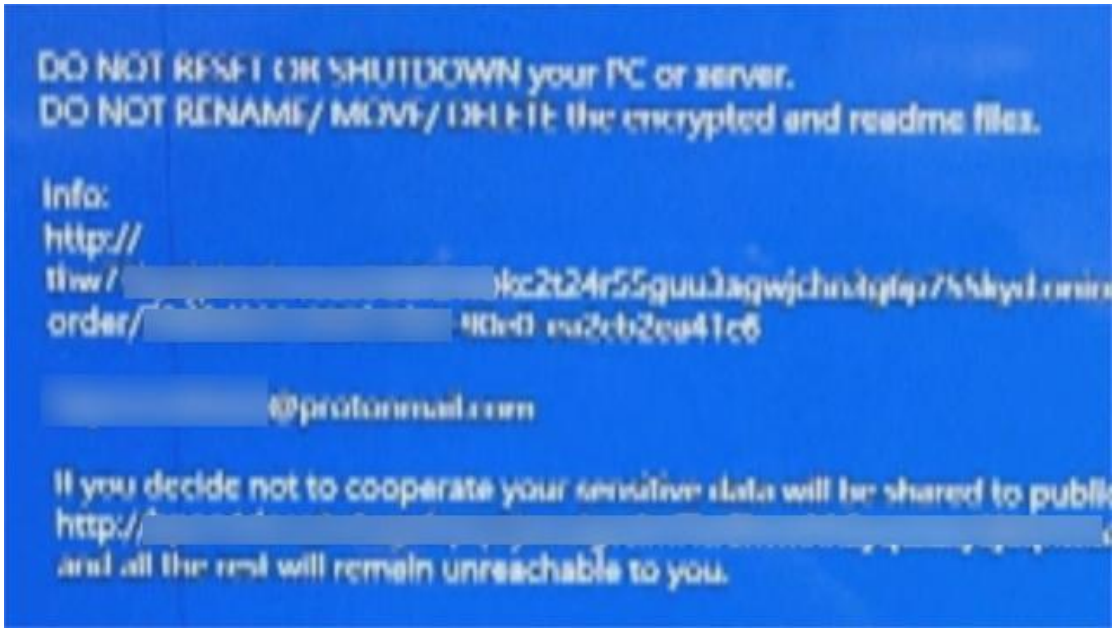
BigBasket 在一份声明中表示：“BigBasket 获悉了潜在的数据泄露事件，并正在与网络安全专家协商并评估解决方案，以评估破坏行为的范围和真实性。我们还向班加罗尔的网络犯罪小组备案，并打算大力追究其罪魁祸首”。（来源：cnBeta）

➢ 全球第二大笔记本电脑制造商仁宝遭到勒索软件攻击

2020 年 11 月 11 日，台湾笔记本电脑电子制造商仁宝在上周末遭受了 DoppelPaymer 勒索软件攻击，攻击者要求将近 1700 万美元的赎金。仁宝是全球第二大笔记本电脑原始设计制造商(ODM)，全球客户涵盖苹果、惠普、戴尔、联想和宏碁等。

攻击者要求 1670 万美元的赎金

上周末，仁宝遭受了网络攻击，但该笔记本电脑制造商声称这只是其办公自动化系统中的“异常”，他们认为这只是系统的安全漏洞问题，而非遭遇勒索软件攻击，仁宝生产线不受网络攻击的影响。但是，周一上班的员工收到仁宝内部发给 IT 部门的一封备忘录表示，要求员工检查工作站的状态并在未受影响的系统上备份重要文件。



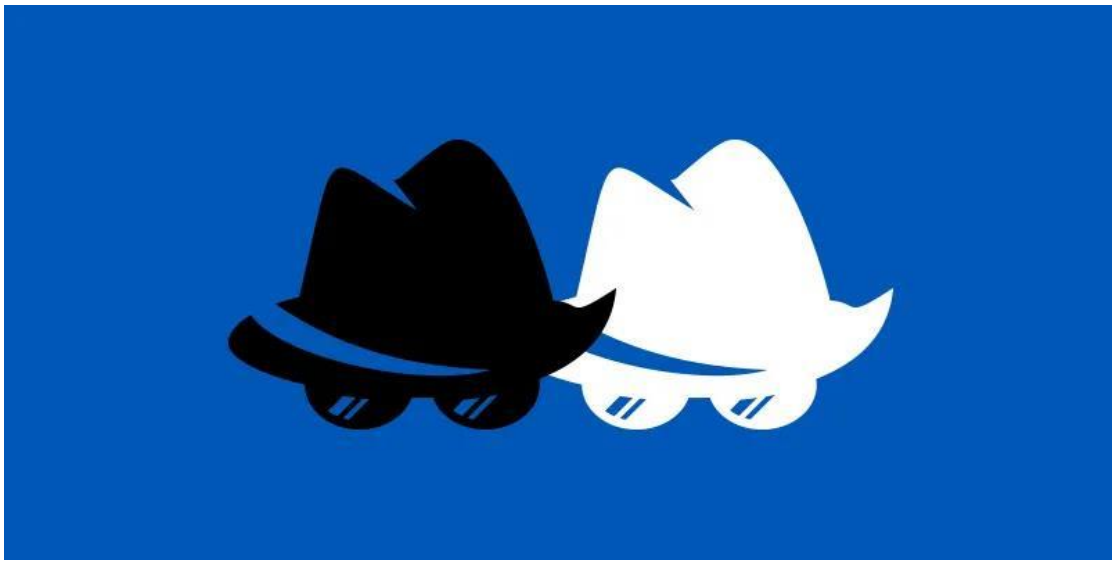
仁宝副总经理卢庆雄说：“主要原因是办公室自动化系统出现异常。我们怀疑遭到黑客入侵，但目前已紧急修复了大部分漏洞，并有望在今天恢复正常。仁宝没有像外界所报道的那样被黑客勒索，目前生产中一切正常。”

但因外媒根据仁宝员工分享的赎金记录的屏幕快照和攻击勒索票据，所以很大可能是遭遇了勒索软件攻击，幕后黑手则是 DoppelPaymer 勒索软件组织。仁宝是今年受勒索软件攻击的第三家台湾主要工厂。台湾国有能源公司 CPC 公司在 5 月份遭到 ColdLocker 勒索软件的攻击，而美国智能手表制造商 Garmin 的台湾工厂在 7 月遭到了 WastedLocker 勒索软件的攻击。（来源：互联网综合整理）

➢ 高中生窃取上亿条公民个人信息 “少年黑客”赔偿并公开道歉

2020 年 11 月 13 日，惠山区人民检察院报道：“希望这次附带民事公益诉讼能让他深刻认识到自己的错误，他以后的人生还很长，要把聪明才智用在正途。”小文的代理律师向检察官表示感谢。这是无锡惠山区人民检察院提起的首个侵犯公民个人信息公益诉讼案。

近年来，侵犯公民个人信息案件呈上升趋势，犯罪者中不乏像小文一样的“少年黑客”，希望通过这起刑事附带民事公益诉讼案，可以对全社会起到教育引导、警示促进的作用。惠山区检察院检察长李营表示。



2018 年 9 月，惠山区警方接到举报称，有人在网上售卖公民个人信息以及盗窃信息所用的黑客软件，经过侦查，警方跨省抓捕了犯罪嫌疑人付某。到案后付某供述，自己售卖的黑客软件都来自一个叫“i 春秋”的网友。经过对“i 春秋”的网络 IP 溯源，警方顺藤摸瓜锁定了住在广东省信宜市的小文，但当侦查人员赶赴广东省找到小文时，发现他竟是一名高三在读学生，到案时刚满 18 周岁。

小文出生于 2001 年，自小就对计算机十分感兴趣，通过自学掌握了编程技术，并编写出一款软件，可以轻松获取百度贴吧用户账号和对应的手机号。在 2018 年 6 月到 7 月的短短一个月时间里，小文就通过自编软件非法获取了约 1 亿条公民个人信息，全部存储于数据库中。小文为了存储获取到的“海量”公民个人信息，专门在境外租用十多台服务器。为了不让其他人发现漏洞，在获取了海量公民个人信息后，小文向百度公司反馈，将网站存在的漏洞进行封堵。

此后，小文在通过微信、QQ 群及境外聊天工具，向他人兜售获取到的公民个人信息，

其中部分交易以比特币为交易货币，共计获利约人民币 2 万元。

2019 年 8 月，惠山区人民检察院以侵犯公民个人信息罪对犯罪嫌疑人小文提起公诉。今年 10 月，该案一审宣判，法院以侵犯公民个人信息罪，对被告人小文判处有期徒刑三年六个月，并处罚金人民币 2 万元。

小文窃取公民个人信息高达 1 亿余条，侵犯了众多公民的信息隐私权，严重损害社会公共利益，在本案审理过程中，惠山区人民检察院向法院提起刑事附带民事公益诉讼，要求小文承担民事赔偿责任，并向社会公众公开赔礼道歉。

今年 10 月，在法院的主持下，双方达成调解协议，“鉴于小文作案时还未成年，案发后充分认识到自己的过错，并且已经承担了相应的民事责任，以调解结案的方式可以节约司法资源，达到更好的社会效果。”该案承办检察官何浦说。（来源：惠山区人民检察院）

➢ 前微软工程师窃取千万美元：自己买车买房，同事做替罪羊

2020 年 11 月 11 日报道，26 岁的 Volodymyr Kvashuk 是一名乌克兰公民，也是前微软工程师。在职两年期间，他以“货币储值”(CSV)的形式(包括礼品卡)从微软窃取了 1000 多万美元的数字资产，最后被判处有期徒刑九年。**根据法院文件显示：**Kvashuk 在 Universal Store Team(UST)时，使用 Microsoft Store 测试帐户进行未经授权的模拟产品购买，并从 Microsoft 窃取了约 1,010 万美元的 CSV 。2018 年 2 月，微软的 UST 欺诈调查罢工团队(FIST)注意到使用 CSV 购买的 Xbox Live 订阅数量出现可疑增长，随后他的恶意行为被发现。

以折扣价出售窃取的 CSV

2016 年 8 月 26 日，Kvashuk 开始在微软工作， 2018 年 6 月 22 日被解雇。被解雇后，他将在职期间盗窃的 CSV 通过折扣价在网上市场转售，至少通过了两个中间转售商 nokeys.com 和 g2a.com。然后，购买 CSV 的第三方可以从 Microsoft 中购买虚拟和实物商品。经 Kvashuk 大量出售后，Microsoft 只能赎回约 180 万美元的 CSV，这意味着微软面临约 830 万美元的财务损失。此外，Kvashuk 使用了 Chipmixer.com 的服务(一种比特币混合服务)来隐藏非法资金的来源，以及在 Paxful 对等加密货币交易平台上使用 Xbox 礼品卡购买比特币。他对账单记录造假，并告诉美国国税局，转移到他账户中的 280 万美元比特币是亲戚送给他的礼物。2018 年 3 月，Kvashuk 购买了一辆大约 16.2 万美元的特斯拉汽车，三个月后，他又以大约 167.5 万美元的价格购买了伦顿湖边的房屋资产。

让同事做替罪羊

最开始 Kvashuk 使用自己的测试帐户非法购买 CSV，此时盗窃了约 12000 美元。随着盗窃金额升级为数百万美元，他开始利用一些同事的帐户来隐藏他的犯罪足迹，并打算误导此后的调查，给出错误的责任人方向。

检察官认为： Kvashuk 的计划每一步都涉及谎言和欺骗。窃取雇主资金已经很糟糕了，但是利用同事的身份犯罪就不仅仅只是偷窃的罪行了。盗取资金、甩锅同事后，他不仅没有承担责任，而且还谎话连篇，没有迹象表明他对自己的罪行感到悔恨。Kvushuk 被判犯有 18 项联邦重罪，其中包括六项洗钱罪名和两项提交伪造纳税申报表的罪名，也被勒令偿还$ 8,344,586 的赔偿。此外，Kvashuk 还可能在其入狱后被驱逐出境。（来源：快科技）

➢ 40 多万条信息泄露圆通回应还“自我表扬”专家：不打老虎没用！

2020 年 11 月 17 日，内部员工与外部不法分子勾结，导致 40 多万条公民个人信息泄露，圆通速递 17 日发布声明并道歉，称系主动发现报案，坚决打击违法行为。**为何圆通的回应给人一种“我发现的、我报案的、我配合参与全过程”的自我表扬感？个人信息泄露频发，究竟有没有办法？对此，中国社科院法学研究所副所长周汉华接受央视《新闻 1+1》采访时进行了解读。**

不应只是道歉该给用户一个说法

近期的一起部督案件中，不法分子与圆通快递多位“内鬼”勾结，通过有偿租用圆通员

工系统账号盗取公民个人信息，再层层将信息倒卖至不同下游犯罪人员。圆通速递 17 日回应称：公司主动发现并报案，犯罪嫌疑人于 9 月已落网。

圆通速递：坚决配合打击涉及用户信息安全的违法行为

圆通速递 V | 11-17 08:34 | 投诉 阅读数：347万+

我们注意到，近日有媒体报道经公司报案、公安机关破获的非法获取并使用快递运单信息的案件。

今年7月底，公司总部实时运行的风控系统监测到圆通速递河北省区下属加盟网点有两个账号存在非该网点运单信息的异常查询，判断为明显的异常操作，于第一时间关闭风险账号，同时立即成立由质控、安保、信息中心、网管以及河北省区组成的调查组，对此事件开展取证调查。调查发现，疑似有加盟网点个别员工与外部不法分子勾结，利用员工账号和第三方非法工具窃取运单信息，导致信息外泄。公司随后向当地公安部门报案，并全力配合调查。相关犯罪嫌疑人于9月落网。更多关于此案件的信息，以公安机关披露的为准。

而早在 2013 年就有媒体曝光，有近百万条圆通快递单个人信息不仅可在网络上购买到，单号数据信息还能 24 小时刷新。对此，中国社科院法学研究所副所长周汉华表示，圆通的回应确实给人“自我表扬”的印象。类似的案子如果发生在发达国家，对于平台公司会有很大冲击。用户是在和平台、圆通打交道，而圆通内部管理上出现了严重问题，所以圆通不应该只是道歉，现在该怎样进行整改、后续有哪些措施，都应该给用户一个说法。

圆通的管理责任执法部门应跟进追究

周汉华认为，圆通公司几名员工外租自己的员工账号，造成了 40 多万条公民个人信息泄露，圆通的内部管理已经存在非常严重的问题。周汉华表示，现有的相关法律法规，包括刑法修正之后，有一条“拒不履行信息网络安全管理义务罪”中有一项具体行为是“致使用户信息泄露，造成严重后果的”，因此行政执法部门，包括刑事执法部门都应该跟进追究相关人员、公司的责任。“拒不履行信息网络安全管理义务罪”这个武器要用，否则这样的事情就会层出不穷。

治理信息泄露不打“老虎”没有用

周汉华表示，国际上现在对于个人信息保护面临一个问题，到底是打“苍蝇”还是打“老虎”？“苍蝇”往往是中下游的，圆通这个案子中的 5 个员工就属于“苍蝇”，平台、大公司就是“老虎”。

专家认为，如果真正要解决个人信息滥用问题，不打“老虎”是没有用的，国际上都是

打“老虎”。“苍蝇”当然也要打，但打“苍蝇”更多是通过治安管理处罚，包括追究刑事责任等。侵犯公民个人信息罪当中的 50 条、500 条、5000 条的标准，对于自然人来说是构成刑事责任了，但这对于“大老虎”来说，是远远不够的。

个人信息为何频频泄露？治理难点何在？

关于侵犯公民个人信息的行为，相关法律法规很多，而且刑法修正案还专门确立了侵犯公民个人信息罪最高刑期是 7 年以下。周汉华认为，现在面临的问题是“牙齿不够锋利”，规定往往处于沉睡状态。“民事维权成本非常大，收益非常低。大家每天都出现这样的问题，都觉得没办法，这是民事维权的困境。”

与此同时，行政执法层面的相关制定也都基本处于休眠状态。周汉华指出，这有非常复杂的原因：首先是取证难，固定证据也难，最后，找到相关的违法链条也很不容易，所以大部分行政执法现在处于休眠状态。现在主要起作用的是公安部门每年通过专项打击行动来进行制裁。因此，周汉华表示，要加大力度打击泄露公民信息的违法行为，对于防范人脸、声音等生物信息泄露，应成为立法、执法的重中之重。（来源：央视新闻）

➢ 中石化“内鬼”修改系统数据偷 1190 万 获刑十五年

2020 年 11 月 18 日报道，加油充值卡是用来为汽车加油的储值卡，因为非常便利，受到广大车主的喜爱，也给不法分子带来了可乘之机。

发现“新”功能 动了歪脑筋

大学毕业的郝某是中石化公司山东分公司财务资产处的一名职员，负责资金管理、客

户往来管理等工作。该公司的加油充值卡系统委托济南某联支付网络服务有限公司(下称济南某联公司)开发。作为一名财务部门的工作人员，郝某和济南某联公司的工程师沟通频繁，掌握了许多加油充值卡系统业务培训资源和信息。

2017 年上半年，郝某被调去做加油充值卡的核算管理和成品油的进货采购业务。在梳理和学习以及与工程师交流的过程中，郝某偶然了解到该系统有一个“特殊调整”功能。设立这个“特殊调整”功能的初衷，是因为在给充值卡充值或者充值卡使用的过程中，有的充值卡没有写进金额导致无法使用，有的充值卡在使用时因顾客对油品不满意要求退货，这时候要求将金额重新写进充值卡，也就是说需要将充值卡的数额进行修改。

这个功能是济南某联公司提供的标准化操作，而山东分公司这些年始终未用过这个功能。2017 年 9 月，郝某无意中了解到系统许多网点(各地的加油站)管理员用户的初始密码没有更改过，就顺手试了一下，发现大部分网点号都能进入系统。于是他选了一家，进入系统后，点击增加了一个新用户，通过“特殊调整”功能向充值卡凭空充值 2000 元，随即退出。为防止被别人发现，他又把新开的用户注销了。

“这样网点的管理员就无法发现有人登录过，第一次我就是想试一试，觉得不一定能成功，就想等一段时间看看有没有问题，会不会被人发现。”郝某交代。

过了一段时间，郝某看没人发现，于是就大胆起来，便登录了济南某联公司的山东加油充值卡自助充值平台，输入上次增加了余额的充值卡卡号，发现充值卡里的确增加了 2000 元，并且也能充到加油卡里。随后，他便用这张加油卡给自己的爱车加油，还用这张卡在加油站的“便利店”里购买了香米和矿泉水等。

虚增假充值 折价真套现

有了第一次的成功，郝某觉得这是个发财的好机会。“因为我本身是干财务的，知道财务只统计网点的售卖和消费，这种‘特殊调整’报表上反应不出来，也就是说不会有人发现。所以我就想通过这种方式多弄点钱。”郝某交代。于是，郝某如法炮制，再次从交易流水里选择消费完毕的充值卡号进行充值，然后到自助充值平台将资金充值到加油卡里。

一段时间过后，依旧没有被人发现，慢慢地，郝某的胆子越来越大。一般几天就操作一次大额充值，每次从几万元到 10 万元，最多时甚至充了 12 万元。他将这些加油卡通过中间人(另案处理)以面值的九二折至九六折不等的价格销售给“黄牛”(另案处理)，后期甚至直接用“黄牛”提供的卡号来充值，赚得是盆满钵满。

核账见异常 虚增上千万

2018 年 6 月，中石化公司山东分公司信息管理处接到该公司零售中心的反映，称该公司预付卡系统资金核对发现了资金异常，有账户资金被人为提升，导致该公司的资金和具体账目不匹配。次日，该公司迅速联系系统开发商济南某联公司，双方一起核对账目，查找漏洞。经过梳理系统数据，业务人员发现第一笔异常额度调整出现在 2017 年 9 月 12 日，后来他们又陆续发现系统中有省内 10 个地市的 15 个发卡点的部分预付费卡的额度出现被提升的情况，累计修改金额为 1900 余万元。

发现这一情况后，该公司紧急冻结了这些预付费卡，冻结金额大约 700 余万元，剩余的资金先前已通过某联支付网上平台充入了 100 余张加油卡中，共计 1190 余万元。公司业务人员继续追查这些加油卡的消费记录，发现自 2017 年 9 月 12 日以来，这些加油卡在安徽、广西两省的 18 个站点和山东 5 个地市的 58 个站点都有消费记录，消费方式主要是加油、购物，且加油卡上的款项几乎消费完毕，总共还剩 40 万元左右。至案发时，该公司直接损失高达 1190 余万元。

非法获暴利 获刑十五年

2018 年 9 月 26 日，济南市历下区公安分局以郝某涉嫌盗窃罪移送历下区检察院审查起诉。今年 3 月，历下区检察院对该案提起公诉。6 月，法院开庭审理此案。庭审中，检察官就被告人郝某及辩护人关于其行为不属于盗窃行为，而是职务侵占行为的辩解作出驳斥：被告人郝某的工作职责中没有权限可以修改加油卡的充值金额，其是通过了解该系统的功能，尝试用不同网点的用户名和猜测使用原始登录密码进入系统，建新账户，设置新密码。郝某使用新建的账户，修改加油卡的金额，符合盗窃罪的犯罪特征，不属于利用其工作职务有关的便利条件。

法院审理后查明，2017 年 9 月至 2018 年 5 月间，郝某在地处济南市历下区的中石化山东分公司，通过尝试登录密码的方式进入中石化加油站多个网点账户系统，将余额为 0 的充值卡金额修改后，再通过自助充值平台将充值卡金额充入加油卡中，先后 179 次修改 113 张充值卡，修改金额为 1900 余万元，其中充入加油卡中的金额为 1190 余万元，加油卡出售后被消费的总额为 1150 余万元。案发后，追回赃款 880 余万元。法院认为，被告人郝某以非法占有为目的，盗窃公私财物，数额特别巨大，其行为已经构成盗窃罪，遂于今年 8 月 23 日，以盗窃罪判处其有期徒刑十五年，并处罚金 10 万元，同时责令其退赔中石化公司经济损失 267 万余元。一审判决后，郝某不服，提出上诉。日前，济南市中级法院对此案作出终审裁定，驳回上诉，维持原判。（来源：检察日报）