国盟信息安全通报

2020 年 8 月 16 日第 222 期

全国售后服务中心

国盟信息安全通报

（第 222 期）

国际信息安全学习联盟

2020 年 08 月 16 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 395 个，其中高危漏洞 120 个、中危漏洞 214 个、低危漏洞 61 个。漏洞平均分值为 5.94。本周收录的漏洞中，涉及 0day 漏洞 184 个（占 47%），其中互联网上出现“wolfSSL 缓冲区过读漏洞、Encode OSS Uvicorn 注入漏洞”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 4221 个，与上周（2739 个）环比增加 54%。

主要内容

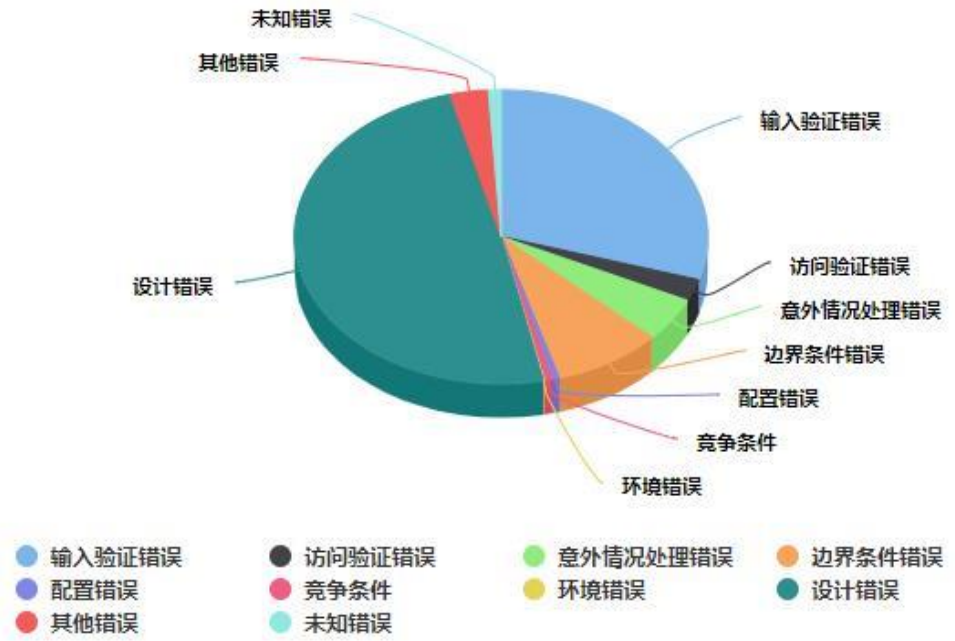
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

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 395 个，其中高危漏洞 120 个、中危漏洞 214 个、低危漏洞 61 个。漏洞平均分值为 5.94。本周收录的漏洞中，涉及 0day 漏洞 184 个（占 47%），其中互联网上出现“wolfSSL 缓冲区过读漏洞、Encode OSS Uvicorn 注入漏洞”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 4221 个，与上周（2739 个）环比增加 54%。

二、安全漏洞增长数量及种类分布情况

➢ **漏洞产生原因（2020 年 08 月 02 日—2020 年 08 月 16）**



➢ 漏洞引发的威胁（2020 年 08 月 02 日—2020 年 08 月 16）

➢ 漏洞影响对象类型（2020 年 08 月 02 日—2020 年 08 月 16）

三、安全产业动态

➢ CNCERT 报告：网络黑产活动呈现专业化趋势

2020 年 8 月 11 日，国家互联网应急中心（CNCERT）编写的《2019 年中国互联网网络安全报告》（以下简称“报告”）正式发布。报告指出，2019 年在我国相关部门持续开展的网络安全威胁治理下，分布式拒绝服务攻击（以下简称 DDoS 攻击）、高级持续性威胁攻击（以下简称 APT 攻击）、漏洞威胁、数据安全隐患、移动互联网恶意程序、网络黑灰色产业链（以下简称黑灰产）、工业控制系统安全威胁总体下降，但呈现出许多新的特点，带来新的风险与挑战。

报告指出，党政机关、关键信息基础设施等重要单位防护能力显著增强，但 DDoS 攻击呈现高发频发态势，攻击组织性和目的性更加凸显，可被利用实施 DDoS 攻击的我国境内攻击资源稳定性持续降低，数量逐年递减，攻击资源迁往境外，处置难度提高。与 2018 年相比，我国境内控制端、反射服务器等资源按月变化速度加快、消亡率明显上升、新增率降低、可被利用的资源活跃时间和数量明显减少——每月可被利用的我国境内活 跃控制端 IP 地址数量同比减少 15.0%、活跃反射服务器同比减少 34.0%。此外，CNCERT/CC 持续跟踪 DDoS 攻击团伙情况，并配合公安部门治理取得了明显的效果。在治理行动的持续高压下，DDoS 攻击资源大量向境外迁移，DDoS 攻击的控 制端数量和来自境外的反射攻击流量的占比均超过 90.0%。攻击我国目标的大规模 DDoS 攻击事件中，来自境外的流量占比超过 50.0%。

针对党政机关、关键信息基础设施等重要单位发动攻击的组织性、目的性更加明显，同

时重要单位的防护能力也显著加强 2019 年，我国党政机关、关键信息基础设施运营单位的信息系统频繁遭受 DDoS 攻击，大部分单位通过部署防护设备或购买云防护服务等措施加强自身防护能力。CNCERT/CC 跟踪发现的某黑客组织 2019 年对我国 300 余个政府网站发起了 1000 余次 DDoS 攻击，在初期其攻击可导致 80.0%以上的攻击目标网站正常服 务受到不同程度影响，但后期其攻击已无法对攻击目标网站带来实质伤害，说明被攻击单位的防护能力已得到大幅提升。

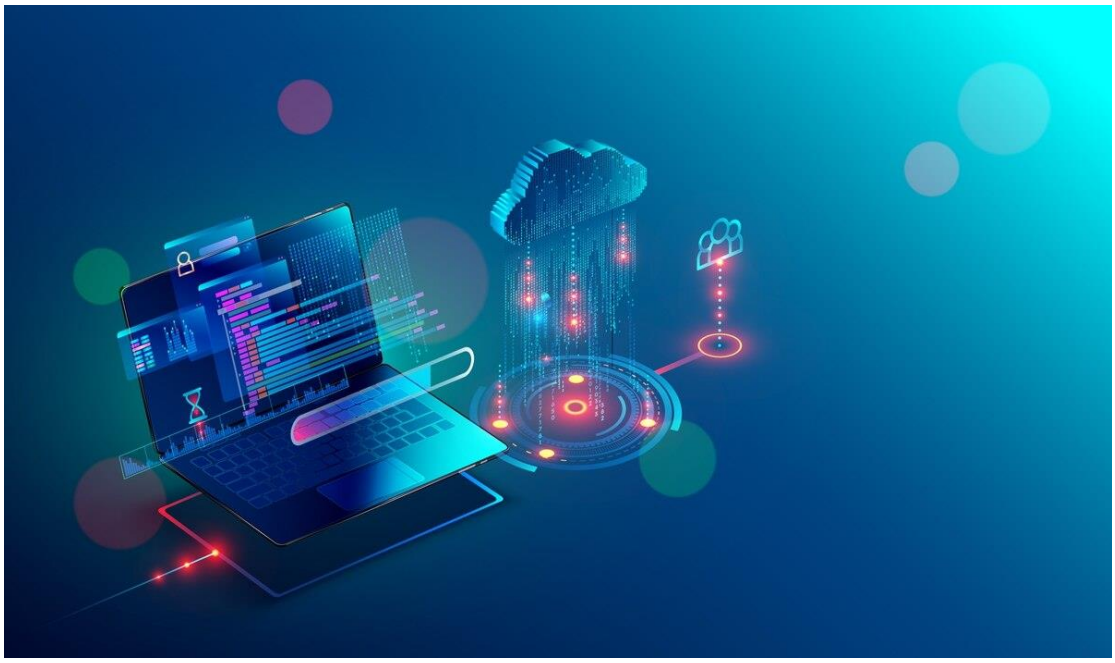
报告显示，2019 年网络攻击领域逐渐由党政机关、科研院所向各重要行业领域渗透。2019 年，我国持续遭受来自“方程式组织”“APT28”“蔓灵花”“海莲花”“黑店”“白金”等 30 余个 APT 组织的网络窃密攻击，国家网络空间安全受到严重威胁。境外 APT 组织不仅攻击我国党政机关、国防军工和科研院所，还进一步向“一带一路”、基础行业、物联网和供应链等领域扩展延伸，电信、 外交、能源、商务、金融、军工、海洋等领域成为境外 APT 组织重点攻击对象。

报告同时指出，以移动互联网仿冒 App 为代表的“灰色”应用程序大量出现，主要针对金融、交通、等重要行业的用户近年来，随着《中华人民共和国网络安全法》《移动互联网应用程序信息服务管理规定》等法律、法规、行业与技术标准的相继出台，我国加大了对应用商店、应用程序的安全管理力度。应用商店对上架 App 的开发者进行实名审核，对 App 进行安全检测和内容版权审核等，使得黑产从业人员通过应用商店传播恶意 App 的难度明显增加，但能够逃避监管并实现不良目的的“擦边球”式的“灰色”应用程序有所增长。例如：具有钓鱼目的、欺诈行为的仿冒 App 成为黑产从业者重点采用的工具，持续对金融、交通、电信等重要行业的用户形成了较大威胁。2019 年，CNCERT/CC 通过自主监测和 投诉举报的方式捕获大量新出现的仿冒 App。

报告提出，网络黑产活动专业化、自动化程度不断提升，技术对抗越发激烈。2019 年，CNCERT/CC 监测发现各类黑产平台超过 500 个，提供手机号资源的接码平台、提供 IP 地址的秒拨平台、提供支付功能的第四方支付平台和跑分平台、专门进行账号售卖的发卡平台、专门用于赌博网站推广的广告联盟等各类专业 黑产平台不断产生。专业化的黑产活动为网络诈骗等网络犯罪活动提供了帮助和支 持，加速了网络犯罪的蔓延趋势。

例如在“杀猪盘”等网盘诈骗犯罪中，犯罪分子通过个人信息售卖的方式获取精准个人信息，从而了解目标人群的爱好特点；通过恶意注册黑产购买社交账号，这些社交账号经过“养号”，具备完整的社交信息，极具迷惑性；通过黑产工具制作团队，快速开发赌博交友网站 App 等诈骗工具。

与此同时，黑产自动化工具不断出现，黑产从业门槛逐步降低。网络黑产工具可自动化进行恶意注册、薅羊毛、刷量、改机等攻击，一般人员经简单学习后即可操作使用。各类专业的网络黑产平台通过 API、易语言模块等方式，提供了标准化接口，网络黑产工具通过调用这些接口集成各类资源，用于网络黑产活动。2019 年监测到各类网络黑产攻击日均 70 万余次，电商网站、视频直播、棋牌游戏等行业成为网络黑产的主要攻击对象，攻防博弈持续演进。



报告提出，随着工业互联网产业的不断发展，互联网侧暴露面持续扩大，新技术的应用给工业控制系统带来了新的安全隐患。例如，2019 年监测发现 的暴露在互联网上的可编程逻辑控制器（PLC）高达 2,583 台，同比增加 8.7%。标 识解析、5G、工业物联网等技术的应用为智能工业赋能，但也将带来信息爆炸、数据泄露等安全隐患，以及海量智能设备的接入和认证管理等安全问题。在工业物联网应用上，大量物联网设备应用在工业领域，涉及智能网关、摄像头、门禁、打印机等多种设备类型。由于物联网设备接入方式灵活、分布位置广泛，其应用打破了工业控制系统的封闭性，带来了新的安全隐患。自 2008 年起，CNCERT 持续编写发布中国互联网网络安全年度报告。（来源：人民网）

- **《2019 年中国互联网网络安全报告》**
- **全文：**https://www.cert.org.cn/publish/main/upload/File/2019Annual%20report.pdf

➢ 解析新版《个人信息安全规范》中的个人信息保护负责人制度

引言：2020 年 3 月 6 日，国家市场监督管理总局、国家标准化管理委员会发布了全国信息安全标准化技术委员会（“信安标委”）编制的《信息安全技术 个人信息安全规范》（GB/T 35273-2020）（“新标准”），该新标准将于 2020 年 10 月 1 日实施，并即将取代已经实施了快两年的 GB/T 35273-2017（“原标准”）。

《网络安全法》出台后，特别是 2018 年 5 月 1 日《信息安全技术 个人信息安全规范》（“旧版规范”）生效以来，不少企业已经搭建起个人信息保护制度框架。数据合规体系是动态的有机体，需要静态的制度框架，更需要合规人员的动态推动，将制度融入商业决策与交易中。即将于 2020 年 10 月 1 日生效的《信息安全技术 个人信息安全规范》（“新版规范”或“《安全规范》”）针对个人信息保护负责人的规定，较旧版规范而言更为具体且务实。

一、为什么要建立个人信息保护负责人制度

个人信息保护负责人是指全面实施统筹组织公司个人信息保护工作、对个人信息安全负直接责任的公司人员。设立个人信息保护负责人对企业落地数据合规制度至关重要。具体而言，科学有效的个人信息保护负责人制度既可提高企业法律风险防御能力，亦可增强其核心竞争力。

（一）提高企业风险防御能力

个人信息保护不力会给企业带来巨大损失：政府调查与处罚轻则迫使企业整改、重则颠覆既有商业模式、甚至导致企业与主要负责人承担刑事责任；个人信息安全事件如果不能及

时、妥善处理，企业所面对的信任危机可能比处罚带来的社会影响更为深远；广大民众不断觉醒的个人信息保护意识更是促使企业时刻不得松懈。个人信息保护负责人既可以帮助企业在日常工作中未雨绸缪又可能在危机事件中力挽狂澜，提高企业防御风险的综合能力。

2017 年 3 月，有消费者认为其个人信息遭到泄露而将某航空公司起诉至法院。法院综合认定被告存在泄露个人信息的高度可能，同时认为法律对经营者采取技术措施和其他必要措施保护消费者个人信息施以强制规定。但是，被告未能证明其已履行法定的个人信息保护义务。2019 年 12 月，同一家航空公司因类似事由被起诉，但法院认为被告在自身掌握信息阶段不存在泄露个人信息的事实。原因在于，航空公司不仅对可查看订单信息的管理系统进行数据脱敏设置，还建立起严密的数据安全管理制度、就数据存储安全进行专门认证、与专业第三方进行合作。

根据公开信息，前述航空公司于 2018 年任命首席数据官，全面负责企业的数据保护与合规运营工作。该航空公司也由此成为国内首家设立数据保护官的企业。[3]虽然任命首席数据官与两份截然相反的判决没有直接关系，但从判决书中航空公司的举证来看，其在一两年间确实就个人信息保护采取了系列技术措施与组织措施，而任命首席数据官不仅是一种合规宣示，对于推动保护措施的落地显然也至关重要。

（二）增强企业核心竞争力

中国企业传统上将法律合规定位为后台支持部门，该等定位在业务拓展特别是开发海外市场时的局限性日益凸显。有能力的个人信息保护负责人有助于树立良好的企业形象，在与监管机构、合作伙伴、甚至竞争对手打交道的过程中，给人以专业、可信的印象，对于增强企业核心竞争力大有裨益。

如何在各国纷繁复杂的法律规定下实现合规，需要个人信息保护负责人的统筹规划。对敏感个人数据加紧审查的国际趋势，尤其是中美经贸摩擦下的监管升级，更是要求企业出海前审慎开展合规评估。华为、蚂蚁金服、360 奇虎等大型企业纷纷设立个人信息保护专家岗位，说明在合规工作进入“深水区”的今天，企业数据合规的水平和深度将直接决定商业机会的获得。

二、如何建立个人信息保护负责人制度

《网络安全法》规定网络运营者应确定网络安全负责人，关键信息基础设施运营者应设置专门的安全管理机构和安全管理负责人。网络安全事关国家安全，而隐私权保护原本侧重私法法益的保护，延展为个人信息保护后则具备更多的公共利益属性，但与网络安全相较仍更突出自主性。在《个人信息保护法》尚未出台的阶段，推荐性的《安全规范》提出设置个

人信息保护负责人制度，起到标准示范作用的同时亦在帮助企业为应对个人信息保护的强制立法做准备。

（一）设置个人信息保护负责人的条件

根据新版规范，当企业（1）主要业务涉及个人信息处理，且从业人员规模大于 200 人；（2）处理超过 100 万人的个人信息，或预计在 12 个月内处理超过 100 万人的个人信息；或（3）处理超过 10 万人的个人敏感信息的，应设置专职的个人信息保护负责人和个人信息保护工作机构。

与旧版规范相比，新版规范对于设置个人信息保护负责人的门槛要求体现出与时俱进和风险导向的趋势。首先，新版规范将处理 50 万人的个人信息提升为 100 万人，与数字经济下企业快速提升的数据处理规模相一致。其次，旧版规范并未将处理个人敏感信息作为标准之一，而新版规范则规定处理超过 10 万人的个人敏感信息即应设立专职的个人信息保护负责人。纵观近年的重点数据执法，往往涉及个人财产信息、生物识别信息、精准的网络浏览记录等个人敏感信息的泄露、非法提供或滥用，故在考虑设置个人信息保护岗位时企业应将是否处理个人敏感信息作为重要参考依据。

前述设置要求亦体现出平衡企业发展与保护法益的合理考虑。第（1）点要求从业人员大于 200 人，说明主要针对中型及以上企业。这样的设定给小微企业的发展留出空间，同时积极引导大中型企业在拓展业务时需更加合规、稳健。第（2）点中的 100 万人构成大城市的常住人口量，收集、处理 100 万人以上的个人信息说明业务已具有相当规模，设置个人信息保护负责人有必要性。

（二）个人信息保护负责人的资质要求

旧版规范生效以来，实务界普遍关注的问题之一是：个人信息保护负责人需要具备何等资质。新版规范分别从经验背景和决策地位两方面，对个人信息保护负责人的资质提出两项指引：

（1）由具有相关管理工作经历和个人信息保护专业知识的人员担任；（2）参与有关个人信息处理活动的重要决策直接向组织主要负责人汇报工作。

根据实践，个人信息保护负责人需要具备法律专业背景，同时能够理解技术、安全对个人信息保护的重要作用。个人信息保护的出发点是确保公司产品及服务符合国内、国际的数据保护法律合规框架，因此对法律的理解是第一准则。由于个人信息保护也涉及数据安全治理，个人信息保护负责人应同时具备国际、国内格局安全观，日常工作中能够与安全和技术人员充分交流并交换意见。显然，传统上此类人才相当稀少，令人欣喜的是近年来出现了一

批对数据保护抱有热忱的专业人士，逐渐形成了中国第一代数据保护人才库。

就决策地位而言，个人信息保护负责人应当具备管理职能，能够参与重要决策。个人信息保护负责人不能仅承担执行责任，也要参与到管理决策，能够与业务部门平等合作、甚至在为公司合规利益把关上有更高的话语权。《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，“数据”已经被纳入市场化配置改革的五大基础生产要素，业务部门为追求盈利，难免在个人信息保护和市场机会的平衡中更偏向市场。同时，相较于业务部门直观反映于短期业绩中的绩效，合规管控更为长远、前瞻，需要时间沉淀才能凸显其价值。因此，个人信息保护负责人需具备管理、决策地位的必要性不言而喻。

（三）个人信息保护负责人的职责

新版规范明确规定了个人信息保护负责人的职责，与旧版规范相比有如下变化：（1）增加的职责为组织制定个人信息保护工作计划并监督落实、公布投诉、举报方式等信息并及时受理投诉举报，以及与监管部门保持沟通，报告个人信息保护和事件处理情况；（2）增强的职责为组织开展个人信息安全影响评估后，还需提出个人信息保护的对策建议，督促整改安全隐患。由此可见，新版规范增加了个人信息保护负责人对外沟通联络的职能，就内部职责而言则更加强调数据合规制度的落地实施。

同时，《安全规范》也非常贴心地为各项职能的具体落实提供建议。其中，新版规范增加的两项内容为个人信息安全工程和个人信息处理活动记录。

个人信息安全工程有些类似 GDPR 项下的 Privacy by Design，即在企业开发具有处理个人信息功能的产品或服务时，根据国家有关标准在需求、设计、开发、测试、发布等系统工程阶段考虑个人信息保护要求，保证在系统建设时对个人信息保护措施同步规划、同步建设和同步使用。因为个人信息安全工程涵盖产品从需求到发布的完整周期，由谁来具体做评估、谁来监督评估、谁来制作个人信息安全影响评估报告等，都由企业根据自身情况决定。不可否认的是，个人信息保护负责人在此过程中会起到重要的作用。《安全规范》建议开展个人信息安全工程时参照国家有关标准，具有很强的现实意义。例如，中国人民银行和全国金融标准化技术委员会发布的《个人金融信息保护技术规范》即要求金融业机构有效隔离开发测试环境和生产环境，在实际开发测试中对个人金融信息进行虚构或者去标识化，且在产品或服务上线发布前进行技术检测。

个人信息处理活动记录与 GDPR 第 30 条的要求较为类似，《安全规范》要求企业建立、维护和更新所收集、使用的个人信息处理活动记录，包括个人信息的类型、数据、来源；根据业务功能和授权情况区分个人信息的目的、使用场景；个人信息出境情况；以及与个人信

息处理活动各环节相关的信息系统、组织或人员。个人信息保护负责人的职能之一即为建立、维护和更新个人信息清单和授权访问策略，正是对应个人信息处理活动记录中的核心部分。

三、完善个人信息保护负责人制度的展望

新版规范完善了个人信息保护负责人制度，企业可以根据自身情况选择适用，为建立数据合规体系奠定基础。我们基于企业的良好实践，为个人信息保护负责人制度、个人信息保护责任体系提出两点展望。

（一）设立个人信息保护工作机构

《安全规范》除要求任命个人信息负责人外，也提到了个人信息保护工作机构。但是，尚未就个人信息保护工作机构给出具体指引。实践中，合规人员在推动数据保护决策时常面临各方阻力，执行中也有不少困难。部分大型公司已经设立数据保护委员会，作为企业数据治理工作的协调机构与最高决策机构，通常由安全技术部、法务部、风险管理部、业务运营部和公共关系部相关管理人员组成。该等设置有助于强化数据保护决策的合意基础，确保决策的顺利推行。特别是当出现安全事件时，数据保护委员会可统筹处理响应、对外进行沟通、适时复盘整改合规措施。

（二）增强个人信息保护负责人的独立地位

新版规范除了开宗明义要求“法定代表人或主要负责人应对个人信息安全负全面领导责任”外，还就个人信息保护负责人的独立性增强了制度保障，即：“应为个人信息保护负责人和个人信息保护工作机构提供必要资源，保障其独立履行职责”。虽然与 GDPR 下 DPO 的独立性仍有所差距，但结合我国的情况以及企业的治理架构，《安全规范》的要求更容易落地实施。企业设计人力制度时，如何确保个人信息保护负责人独立、专业、不受无关干扰做出正确合理的决策，是企业长远发展的一项重要考量。（来源：全国信息安全标准化技术委员会）

➢ 首部关于数据交易的地方性立法即将颁布，这 8 点需引起注意

习近平总书记指出：“安全和发展是一体之两翼、驱动之双轮”，“要处理好安全和发展的关系，做到协调一致、齐头并进，以安全保发展、以发展促安全”。保障数据安全和促进数据开发利用，是新时代背景下建设网络综合治理体系的关键，也是提升国家治理体系和治理能力现代化水平的重要手段。当前是我国数据法律制度建设的黄金期。

2020 年 7 月 3 日全国人大常委会法工委公布了《数据安全法（草案）》（以下简称《数

安法草案》），《数安法草案》坚持安全与发展并重，不仅规定了诸多数据安全方面的法律制度，而且就数据开发利用、大数据、数据交易等制度也做了规定。《数安法草案》公布后进一步激发了大批地方立法，截止 8 月 5 日，已有三部地方性数据立法向社会首次公开征求意见（见表 1），这些立法在《数安法草案》公开征求意见期间同步征求意见，具有很强的央地互动、制度探索意义，也说明了数据法律建设的必要性和急迫性。

法规名称	起草单位	公布时间	章节条目
《中华人民共和国数据安全法（草案）》	全国人大常委会法工委	7月3日	7章51条
《安徽省大数据发展应用条例（草案征求意见稿）》	安徽省司法厅	7月6日	7章46条
《深圳经济特区数据条例（征求意见稿）》	深圳市司法局	7月15日	7章103条
《天津市数据交易管理暂行办法（征求意见稿）》	天津市互联网信息办公室	7月30日	9章40条

天津地位特殊，从 2016 年开始天津就作为京津冀大数据综合试验区的重要参与方，近年来在数据治理建章立制方面做出了诸多探索，比如 2017 年发布了《天津市运用大数据加强对市场主体服务和监管的实施方案》，2018 年发布了《天津市促进大数据发展应用条例》，2019 年发布了《天津市大数据发展规划(2019—2022 年)》《天津市数据安全管理办法（暂行）》等行政规范性文件。今年 7 月 30 日公布了《天津市数据交易管理暂行办法（征求意见稿）》（以下简称《办法》），这一系列文件已逐渐搭建起了天津数据治理架构。本文就学习《办法》的收获谈几点思考，并对其中的部分内容提出完善建议，以与相关立法机关、专家学者交流探讨。

一、《办法》在制定适合国情和数据特点的交易制度方面具有探索性意义

今年初，工业和信息化部发布《2020 年大数据产业发展试点示范项目名单公示》，全国遴选出的 200 个试点示范项目中，天津十家企业入选，排名位居全国第二，天津大数据产业取得显著成果。

数据是数字经济时代的石油。数据要发挥要素作用就必有充分自由流通的渠道，数据交易是数据治理必不可少的核心内容。《数安法草案》在第十七条、第三十条对数据交易制度进行了规定。其中第十七条规定：“国家建立健全数据交易管理制度,规范数据交易行为，培

育数据交易市场”。第三十条规定：“从事数据交易中介服务的机构在提供交易中介服务时，应当要求数据提供方说明数据来源,审核交易双方的身份，并留存审核、交易记录”。这两个条款的优点是体现了国家立法层面对于数据交易的宏观统筹，缺点是过于概括可操作性不足。

《办法》作为我国第一部专门对数据交易进行规范的地方性立法，在探索适合我国国情和数据特点的交易制度方面具有重要意义，其一方面可为《数安法草案》的完善提供地方经验，另一方面也会给其他地方数据立法提供借鉴。后文着重对《办法》尚待完善之处提出建议供参考。

二、《办法》将数据交易限定在专门的数据交易服务机构的做法需评估对交易自由的影响

根据《办法》第二、六、七条的规定，《办法》将数据交易方式限定为只能在专门的数据交易服务机构进行，排除了其他交易方式，其好处是一定程度上有助于提高数据交易的可信度、专业化、规范化水平，并方便监管机构监管；其可斟酌之处是单一的交易方式恐难以适应交易市场多样化的交易需求。

《办法》的规定与目前一些地方立法不一致,后者一般采取鼓励、倡导的态度，不强制要求在专门的数据交易服务机构进行数据交易（见表 2）。

序号	地方性立法	条款
1	《贵州省大数据发展应用促进条例》	第十九条 鼓励和引导数据交易当事人在依法设立的数据交易服务机构进行数据交易。
2	《天津市促进大数据发展应用条例》	第三十三条 鼓励和引导数据交易当事人在依法设立的数据交易服务机构进行数据交易。
3	《安徽省大数据发展应用条例（草案征求意见稿）》	第二十四条 鼓励和引导数据交易当事人在依法设立的大数据交易服务机构进行数据交易。
4	《深圳经济特区数据条例（征求意见稿）》	第五十八条 数据要素市场主体应当遵循自愿、公平和诚实信用的原则开展数据交易活动。数据要素市场可采用自主交易、交易平台等多种合法方式开展数据交易活动，引导数据要素市场主体通过依法设立的数据交易平台进行数据交易。支持数据交易技术研发和创新数据交易模式，拓宽数据交易渠道，促进数据高效流通。

从国外看也没有限制单一的交易方式。例如，2018 年欧盟发布的《关于欧洲企业间数据共享的研究》总结了实务中数据交易的五种方式（见表 3）。

序号	交易方式	内容
1	数据货币化	是指公司在经过个人适当许可的前提下，通过与其他公司共享数据而取得额外收入的方法，即公司公司之间直接交易。
2	数据市场	是指数据交易中通过建立安全的在线平台，使数据供方和数据需方在平台上进行数据交易。在这种情况下，管理数据市场的公司通过数据交易获取收益。
3	行业数据平台	是指为了促进公司间数据共享的协作而创建，如公司为了促进新产品/服务的开发、提高其内部效率，而自愿选择加入一个封闭、安全和专属的平台，以便共享数据。在这种环境下，数据通常免费共享（也有的付费共享）。
4	技术支持者	是指作为数据共享过程中的第三方，专门从事并致力于通过技术解决方案实现数据共享。
5	开放数据策略	指采用公司间开放数据政策，也包括政府开放数据平台。

《关于构建更加完善的要素市场化配置体制机制的意见》提出“促进要素自主有序流动”，建议在数据交易过程中尊重市场主体的意愿，保障私法自治精神，在交易方式上保持一定开放性。

三、《办法》将“可交易数据”限定为“无法识别特定数据提供者且不能复原”的做法压窄了数据交易的范围

数据交易的范围是数据交易的重大问题，既与交易安全息息相关，也与交易效率密切相连。《办法》第十四条规定“依法获取的各类数据经处理无法识别特定数据提供者且不能复原的，可以交易”，将“可交易数据”限定为“无法识别特定数据提供者且不能复原”的数据。这一限定缩减了可供交易的数据，出发点可能是保障安全，但也使大量数据难以通过交

易发挥价值。《网络安全法》等上位立法，部分地方立法以及国家标准的相关规定均未作出上述限定（见表 4）。故对“可交易数据”限定宜慎重，建议对不同类型交易标的设定不同交易要求，提出不同的安全保障义务，以充分保障不同类型数据的交易安全需求。

四、《办法》规定了数据交易服务机构应当承担七项义务，该义务显得过重或导致增加交易难度

这些义务具体包括：

- 组织并监督数据交易、结算和交付；
- 对数据供方提供的数据来源合法性进行审核；
- 对数据违规使用行为进行监测；
- 制定并执行交易违规处罚规则；
- 对数据交易服务平台进行管理；
- 受理解决有关数据交易的投诉；
- 法律法规规定的其他应履行义务。

其中第二项关于对数据供方提供的数据来源合法性进行审核的义务难度相对过高，对数据交易服务机构压力较大，建议增大交易双方的安全保障义务；第四项赋予了数据交易服务机构制定并执行交易违规处罚规则，然而其作为服务机构似并无处罚数据交易双方的行政权力，后续还要结合对数据交易服务机构性质的进一步研判进行分析。

五、《办法》规定的数据交易条件过于严格给交易带来不确定性

《办法》对数据交易双方应满足的条件提出了不同要求。通过比较分析发现：《办法》对“数据供方”和“数据需方”均提出了“一年内无重大数据类违法违规记录”的要求，这一要求与国家推荐性标准《信息安全技术数据交易服务安全要求》第 5.1 条和 5.2 条的要求近似，但依然存在一定不足。

一是本条近似于设定了数据供方的交易资质和市场准入门槛，使得不具备相应资质要求则不能交易数据。

二是当市场主体发生重大数据类违法违规记录以后，将在一年内不能进行数据交易，责罚显得过重。

三是数据交易是民事主体之间自由开展的民事行为而非行政行为，因为一项行政违法行为就面临“禁止”数据交易的困境，对于市场主体尤其是以数据交易为业的市场主体而言具有重大不利影响。

在当前保护主义上升、世界经济低迷、全球市场萎缩的外部环境下，“新冠肺炎疫情对

我国经济和世界经济产生巨大冲击，我国很多市场主体面临前所未有的压力。市场主体是经济的力量载体，保市场主体就是保社会生产力”，建议给予市场主体从事数据交易充分的法治保障和制度激励。

六、《办法》禁止数据需求方转交易的规定过于绝对化

《办法》第十一条规定：“数据需方无权将交易数据转让给第三方”，禁止数据需方在数据交易后向第三方转交易。从控制风险角度看，有些类型数据禁止转交易或具有合理性，但禁止所有数据转交易则显得过于绝对。这种一刀切的弊端是使得数据需方从数据供方获得的权益内容非常有限，性质上近似于只获得了一项普通许可，排除了直接获得数据控制权的可能，可享有的数据权益较为有限，不利于激发其数据交易的积极性及数据交易市场活力。建议在保障安全的前提下保留转交易的可能。

七、《办法》有关政务数据交易的规定不够自洽

《办法》第十四条规定：“鼓励、支持通过数据交易的方式依法开发利用政务数据和社会数据”。第八条在有关数据供方的规定中明确提出：“行政机关及法律法规授权的具有管理公共事务职能的组织不得作为数据供方参与数据交易”，但在第九条有关数据需方的要求无此类限制。据此似可推出如行政机关及法律法规授权的具有管理公共事务职能的组织作为交易方参与数据交易，则只能以数据需方的身份参与数据交易，不能提供数据而只能接受数据。这对于促进政务数据开放利用激励不足。建议删除第八条对数据供方不能为“行政机关及法律法规授权的具有管理公共事务职能的组织”的限定。

八、不断加强对数据交易安全的保障

数据交易法律制度建设的底线是保障数据安全，目标是发挥数据交易对经济增长的推动作用，满足人民群众在数字经济时代下对美好生活的向往。平衡“数据发展”与“数据安全”是数据治理领域的永恒难题。

《办法》从“数据交易”角度对“数据发展”进行了探索，并规定了相应安全管理制度保证发展。但也有部分论证不充分的地方，其落地出台将对市场主体数据交易活动产生重大影响。数据交易性质上属于商业活动，商业活动天然需要统一的市场规则。如各省（区、市）都建立了自己的数据交易规则，而且这些交易规则却各不相同，恐对数据交易活动产生负面影响。

《数安法（草案）》关于数据交易管理制度建设主体已经明确为国家主导，建议后续相关立法中以国家有关数据交易管理规定为依据，在允许范围内进行细化，推动建立安全、高效、全国统一的数据交易规则。（来源：腾讯安全战略研究）

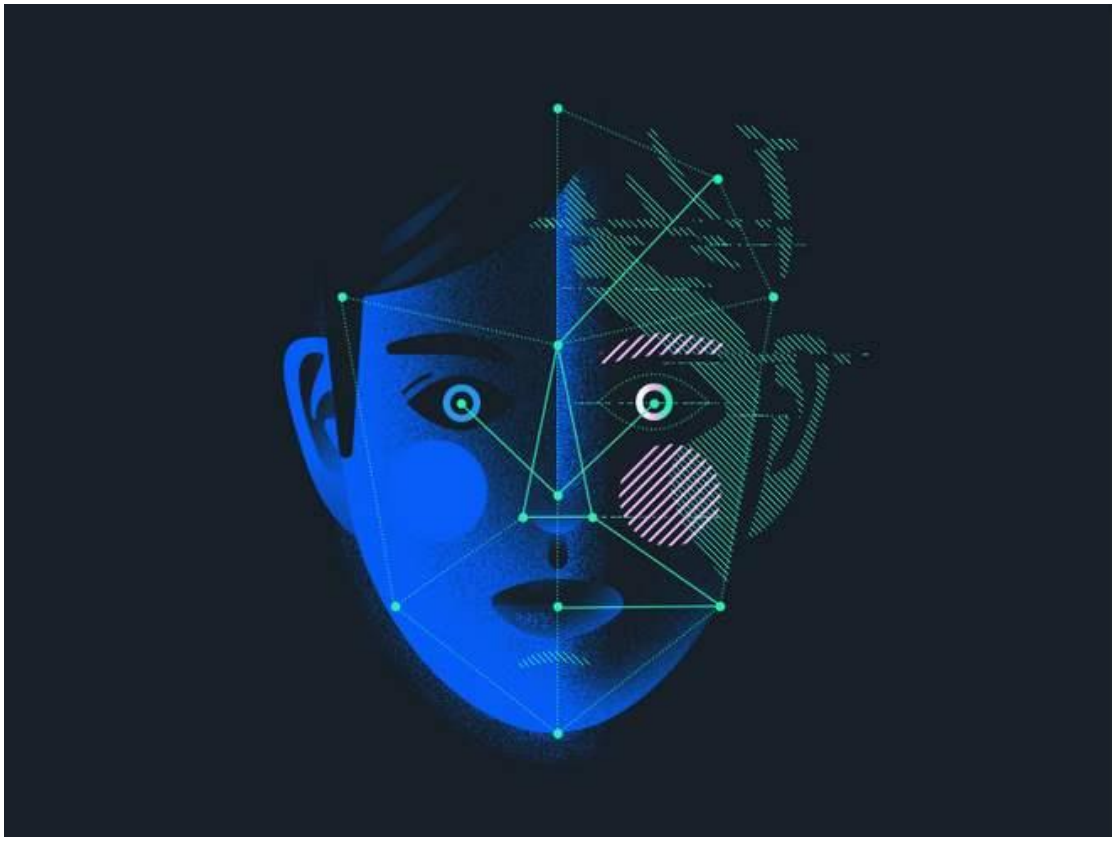
➢ 滥用人脸识别存信息安全隐忧

点完餐看一下摄像头就能完成支付，住酒店刷脸后才能登记，上公厕用厕纸也得刷个脸才能取。随着人工智能的发展，人脸识别技术得到广泛应用，“脸”的应用场景被不断拓宽。

人脸识别技术看似“高大上”，但其存在的个人生物信息被过度采集和滥用的风险也不容忽视。相关专家表示，人脸识别技术不是万能的，收集、处理个人信息应当遵循合法、正当、必要的原则，基于身份验证等需要收集相关信息后也应尽到严格保管的责任和义务。中央网信办等部门近期也表示，针对面部特征等生物特征信息收集使用不规范等重点问题，App 专项治理工作组将开展专题研究。

人脸识别应用场景不断拓展

在屏幕上点餐，选择刷脸支付，人脸比对后，输入手机号码后四位就完成付款。在上海一家商场的肯德基餐厅，记者观察发现，使用自助点餐机点餐的顾客中，选择“刷脸支付”的消费者占到两至三成。



除了大商场、大超市，在部分便利店和街边小店里，刷脸支付设备也得到广泛应用。在上海陕西南路一家便利店，市民洪浩晨在购买一瓶饮料后，通过刷脸方式完成付款。“从去年开始用刷脸支付就比较多，感觉比二维码方便。”洪浩晨说。

除了消费领域的便利支付，身份认证是人脸识别技术的另一大主战场。在全国机场和火车站的部分通道，乘客将身份证放在相应感应区，面部正视摄像头，每人只需几秒钟就可完成相关信息核验，快速进站。

一些公共服务机构还利用人脸识别技术来打击“黄牛”。复旦大学附属肿瘤医院一半以上的患者来自外省份甚至境外，该院去年就推出“人脸识别+身份绑定”系统，强化早高峰时段热门专家（特需）现场号源的管理。通过人脸识别系统绑定挂号人的身份，使得号贩子失去了现场“投机挂号”的操作空间。

“考虑到家属、亲友代挂号的情况，我们还设定每位患者可以绑定一位代挂号人身份认证信息。”复旦大学附属肿瘤医院门诊办公室主任董枫说。

不仅是医院，记者发现，各地政务类 App 中，刷脸登录、人脸验证也已经广泛使用，如某地公积金 App，用户就可通过人脸识别完成验证，进行线上支取公积金。上海市民胡志国说：“年纪大了，密码经常忘，尤其是登录一些不常用的 App 时都需要重置密码，刷脸就不存在这个问题。”

人脸识别是不是用得太多了？

不可否认，在人工智能成为新基建的背景下，人脸识别技术有其先进性和高效率。但任何先进技术的应用，都有其边界。在一些不必要的场景下，让渡自己的隐私，来换取一张通行证，必然会引发其他方面的问题。

“现在上班刷脸打卡，工作时刷脸打开手机、笔记本电脑，午饭时刷脸支付，出差住酒店也得刷脸登记，甚至上公厕取厕纸都要刷脸，这张老脸是越刷越多，总感觉不对劲。”有网友如此感慨。

——强制刷脸遭质疑。记者梳理发现，关于公共场合使用人脸识别技术的争议和投诉正在增多。在合肥市“12345 政府服务直通车”上，7 月份有市民投诉：“繁华逸城”小区更换新物业后，办理门禁卡强制要求采集业主人脸信息。

对此，肥西县政府回复称，该项目的初衷是创建智慧平安小区，系统最终接入公安后台。“考虑老人和儿童人像采集不方便，可以办理门禁卡。”

上海一居民小区近期将小区门禁系统改为人脸识别系统。小区居民王女士说，改造前所有住户均需到物业采集人脸信息，“其实大家对采用人脸识别系统还是认可的，只是不知道个人信息是否会得到很好的保护。物业为了让大家放心，出具了一份承诺书，承诺将严格保存收集的相关信息。”

——技术能力参差不齐。丰巢快递柜此前曾试点“刷脸取件”，其后被发现使用打印的

取件人照片，也可以轻而易举地刷脸打开快递柜取件。丰巢回应称，“刷脸取件”功能仅为小范围试运营，并将测试版下线。

据悉，人脸识别技术可粗略分为基于 2D 人脸图像的技术和基于 3D 人脸图像的技术。通过照片即可完成人脸验证，大概率是采用了技术门槛较低的 2D 人脸图像认证。中国物流学会特约研究员杨达卿说，快递物流行业涉及消费者个人信息和财产，推广使用新技术时应慎之又慎。

——信息安全存隐忧。“密码泄露了，可以换一个，这脸部信息要是泄露了，可怎么换啊？”不少网友表示。

北京大学法学院教授薛军表示，人脸信息作为生物识别信息，一般来说伴随着人的一生，是不可更改的。这与手机号码之类的个人信息不一样，后者发生泄露，实在不行还可以换一个。但人脸信息发生泄露，不太可能去“换脸”。

不宜普遍适用

人脸识别技术虽然有其优势，但并不能在生活各个领域普遍适用，更不能在部分商业领域强制使用。北京志霖律师事务所律师赵占领认为，收集使用个人信息，需要遵循三个原则，也就是合法、正当、必要原则，但目前缺少判断必要性的标准和依据。“目前收集人的脸部特征信息的商业机构，大多数是基于身份验证的需要。在企业收集这类信息后，能不能妥善保管并按照事先所告知的方式去使用相关信息，这也是大家最为担心的。”

薛军认为，利用人脸信息来快速、精确识别个人主体，对于个人行动轨迹的追踪非常高效，但因此对个人隐私权可能带来的侵害，也非常严重。

中国政法大学传播法研究中心副主任朱巍说，对收集个人生物信息的管理，核心在于对获取方的管理。“现实中遵循的原则应当是能不采集个人生物信息就不采集，而且宜通过立法，进一步明确具备采集资格的主体范围。消费者面对商家，也应当有控制、注销已被采集的生物信息的权利。”（来源：经济参考）

四、政府之声

➢ 五部门印发《国家新一代人工智能标准体系建设指南》

2020 年 8 月 5 日，国家标准委、中央网信办、国家发改委、科技部、工信部五部门联合发布《国家新一代人工智能标准体系建设指南》（以下简称《指南》），以加强人工智能领域标准化顶层设计，推动人工智能产业技术研发和标准制定，促进产业健康可持续发展。业内人士指出，“当前我国车联网、智能交通等新兴产业的发展处于加速期，迫切需要标准化工作的支撑和引领，《指南》的发布恰逢其时。”

《指南》提出，到 2021 年，明确人工智能标准化顶层设计，研究标准体系建设和标准研制的总体规则；明确标准之间的关系，指导人工智能标准化工作的有序开展，完成关键通用技术、关键领域　技术、伦理等 20 项以上重点标准的预研工作。

《指南》明确，到 2023 年，初步建立人工智能标准体系，重点研制数据、算法、系统、服务等重点急需标准，并率先在制造、交通、金融、安防、家居、养老、环保、教育、医疗健康、司法等重点行业和领域进行推进。建设人工智能标准试验验证平台，提供公共服务能力。（来源：国家市场监督管理总局）

- **《国家新一代人工智能标准体系建设指南》**
- **全文：**http://gkml.samr.gov.cn/nsjg/bzjss/202008/t20200805_320544.html

➢ 《信息安全技术关键信息基础设施安全防护能力评价方法》等标准征求意见

2020 年 8 月 10 日，全国信息安全标准化技术委员会归口的《信息安全技术关键信息基础设施安全防护能力评价方法》等 2 项国家标准（清单见附件）现已形成标准征求意见稿。

根据《全国信息安全标准化技术委员会标准制修订工作程序》要求，现将该 2 项国家标准（征求意见稿）面向社会公开征求意见。（来源：全国信息安全标准化技术委员会）

➢ 中央网信办、教育部联合启动涉未成年人网课平台专项整治

2020 年 8 月 7 日，目前，网络“云课堂”已成为广大学生疫情期间学习的主渠道，但一些网站平台无视社会责任，屡屡利用网课推广网游、交友信息，甚至散布色情、暴力、诈骗信息，危害广大学生特别是未成年人身心健康，社会影响十分恶劣。

为切实解决涉未成年人网课平台突出问题，维护未成年人合法权益，促进网课平台规范有序发展，中央网信办、教育部决定即日起启动为期 2 个月的涉未成年人网课平台专项整治。

此次专项整治将聚焦网民反映强烈的突出问题，在不同环节开展治理。开设未成年人网课的各类网站平台，必须切实承担信息内容管理主体责任；要对课程严格审核把关，确保导向正确；开设评论互动功能要建立信息内容“先审后发”制度；要加强网课页面周边生态管理，不得出现危害未成年人身心健康的内容；不得利用弹窗诱导点击不适宜未成年人的页面；不得推送与学习无关的广告信息；不得利用公益性质网课谋取商业利益。

有关负责人表示，管理部门对利用网课损害未成年人权益的不法行为采取“零容忍”态度，在专项整治期间，各地网信部门、教育行政部门将进一步加大对涉未成年人网课平台违法违规行为的执法处罚力度，按照露头就打、从严从重原则，依法处置违法违规网站平台和相关机构，为未成年人营造积极健康的网络学习环境。（来源：中国网信网）

➢ 工信部发布《电信和互联网行业数据安全标准体系建设指南（征求意见稿）》

2020 年 8 月 11 日，工信部公开征求对《电信和互联网行业数据安全标准体系建设指南（征求意见稿）》的意见。

《电信和互联网行业数据安全标准体系建设指南（征求意见稿）》（以下简称《建设指南》）指出，到 2021 年，将初步建立电信和互联网行业数据安全标准体系，有效落实数据安全管理要求，基本满足行业数据安全保护需要，推进标准在重点企业、重点领域中的应用，研制数据安全行业标准 20 项以上。到 2023 年，健全完善电信和互联网行业数据安全标准体系，

标准技术水平、应用水平和国际化水平显著提高，有力促进行业数据安全保护能力提升，研制数据安全行业标准 50 项以上。

据悉，《建设指南》包括建设思路及目标、建设内容、组织实施三个部分。

一是建设思路及目标。明确了电信和互联网行业数据安全标准体系建设的总体思路、基本原则、建设目标。

二是建设内容。提出了电信和互联网行业数据安全标准体系框架、数据安全重点标准化领域及方向，具体为基础共性、关键技术、安全管理、重点领域四大类标准。其中，基础共性标准包括术语定义、数据安全框架、数据分类分级，可为各类标准制定提供基础性支撑。关键技术标准从数据采集、传输、存储、处理、交换、销毁等数据全生命周期维度对数据安全技术进行规范。安全管理标准从数据安全框架的管理视角出发，指导行业有效落实相关法律法规对数据安全管理的要求，包括数据安全规范、数据安全评估、监测预警与处置、应急响应与灾难备份、安全能力认证等标准。重点领域标准结合相关领域的实际情况和数据安全保护的具体要求，指导行业有效开展重要领域数据安全保护工作。

三是组织实施。通过实施动态更新、推进标准研制、加强宣贯实施、加强国际合作四方面工作，为做好电信和互联网行业数据安全标准化工作提供坚实保障。此外，《建设指南》还对术语定义和已发布、制定中、拟制定的数据安全相关标准进行了梳理，形成《数据安全相关标准项目明细表》，供各方进行参考。

《建设指南》显示，结合当前电信和互联网行业数据安全面临的形势和挑战，梳理近年来已发布和制定中的百余项数据安全相关标准，目前数据安全标准化工作仍存在三大问题。一是标准体系性不强，标准制定工作缺乏统筹协调，术语定义、分类分级等基础性标准尚不完善。二是部分关键标准亟需制定，数据安全评估、重要数据保护等重点标准进展缓慢。三是部分重点领域相关标准仍存在空白，数据安全标准对 5G、移动互联网、车联网、物联网、工业互联网、云计算、大数据、人工智能、区块链等重点领域高质量发展的支撑作用有待加强。（来源：中华人民共和国工业和信息化部）

- **电信和互联网行业数据安全标准体系建设指南（征求意见稿）**
- **全文：**http://www.miit.gov.cn/n1278117/n1648113/c8050746/content.html

五、本期重要漏洞实例

➢ Microsoft 发布 2020 年 8 月安全更新

发布日期：2020-08-11

更新日期：2020-08-11

描述：8 月 11 日，微软发布了 2020 年 8 月份的月度例行安全公告，修复了其多款产品存在的 120 个安全漏洞。受影响的产品包括：Windows 10 2004 & WindowsServer v2004（86 个）、Windows 10 1909 & WindowsServer v1909（86 个）、Windows 10 1903 & WindowsServer v1903（85 个）、Windows 8.1 & Server 2012 R2（57 个）、Windows RT 8.1（56 个）、Windows Server 2012（40 个）、Microsoft Edge (EdgeHTML-based)（3 个）、Internet Explorer（3 个）和 Microsoft Office-related software（18 个）。利用上述漏洞，攻击者可绕过安全功能限制，获取敏感信息，提升权限，执行远程代码，或进行拒绝服务攻击等。CNVD 提醒广大 Microsoft 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

CVE 编号	公告标题和摘要	最高严重等级和漏洞影响	受影响的软件
CVE-2020-1472	**.NET Framework 远程代码执行漏洞** Microsoft .NET Framework 处理输入时存在远程代码执行漏洞。成功利用此漏洞的攻击者可以控制受影响的系统。 要利用此漏洞，攻击者需要能够将构建的文件上传到 web 应用程序。 安全更新通过更正.NET Framework 处理输入的方式来解决该漏洞。	严重 特权提升	Server 2019 Server 2016 Server, version 2004 Server, version 1909 Server, version 1903 Server 2012 Server 2012 R2
CVE-2020-1464	**Windows 欺骗漏洞** 当 Windows 错误地验证文件签名时，存在欺骗漏洞。成功利用此漏洞的攻击者可以绕过安全功能并加载未正确签名的文件。 在攻击场景中，攻击者可以绕过旨在防止加载未正确签名的文件的安全功能。 该更新通过更正 Windows 验证文件签名的方式来解决该漏洞。	重要 欺骗	Windows 10 Server 2019 Server 2016 Server, version 2004 Server, version 1909 Server, version 1903 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-1554	**Media Foundation 内存破坏漏洞** 当 Windows Media Foundation 未能正确地处理内存中的对象时，存在内存破坏漏洞。成功利用此漏洞的攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。 攻击者可以通过多种方式利用此漏洞，例如说服用户打开构建的文档，或说服用户访问恶意网页。 安全更新通过更正 Windows Media Foundation 如何处理内存中的对象来解决此漏洞。	严重 远程执行代码	Windows 10 Server 2019 Server 2016 Server, version 2004 Server, version 1909 Server, version 1903 Windows 8.1 Server 2012 Server 2012 R2

CVE-2020-1585	**Microsoft Windows Codecs Library 远程代码执行漏洞** Microsoft Windows Codecs Library 处理内存对象的方式存在远程代码执行漏洞。成功利用此漏洞的攻击者可以控制受影响的系统。然后，攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。 利用此漏洞需要程序处理构建的图像文件。 此更新通过更正 Microsoft Windows 编解码器库如何处理内存中的对象来解决此漏洞。	严重 远程执行代码	Windows 10
CVE-2020-1509	**Local Security Authority Subsystem Service 提升权限漏洞** 当经过身份验证的攻击者发送构建的身份验证请求时，Local Security Authority Subsystem Service (LSASS) 中存在权限提升漏洞。成功利用此漏洞的远程攻击者可能会导致目标系统的 LSASS 服务的权限提升。 安全更新通过更改 LSASS 处理构建的身份验证请求的方式来解决该漏洞。	重要 特权提升	Windows 10 Server 2019 Server 2016 Server, version 2004 Server, version 1909 Server, version 1903 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-1567	**MSHTML Engine 远程代码执行漏洞** MSHTML Engine 未能正确地验证输入时存在远程代码执行漏洞。攻击者可以在当前上下文中执行任意代码。如果当前用户使用管理用户权限登录，成功利用此漏洞的攻击者可以控制受影响的系统。然后，攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。 在 HTML 编辑攻击场景中，攻击者可以诱骗用户编辑编制的文件，该文件旨在利用此漏洞进行攻击。 安全更新通过修改 MSHTML 引擎验证输入的方式来解决该漏洞。	严重 远程执行代码	Internet Explorer 11 Internet Explorer 9
CVE-2020-1380	**Scripting Engine 内存破坏漏洞** Scripting Engine 在 Internet Explorer 中处理内存中的对象时存在远程代码执行漏洞。该漏洞可能会破坏内存，从而使攻击者能够在当前用户的上下文中执行任意代码。成功利用此漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理用户权限登录，成功利用此漏洞的攻击者可以控制受影响的系统。然后，攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。 安全更新通过修改脚本引擎处理内存中对象的方式来解决该漏洞。	严重 远程执行代码	Internet Explorer 11
CVE-2020-1483	**Microsoft Outlook 内存破坏漏洞** 当软件未能正确处理内存中的对象时，Microsoft Outlook 存在远程代码执行漏洞。成功利用此漏洞的攻击者	严重 远程执行代码	Office 2019 365 Apps Enterprise Outlook 2016

	可以在当前用户的上下文中运行任意代码。如果当前用户使用管理用户权限登录，攻击者可以控制受影响的系统。然后，攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。与使用管理用户权限操作的用户相比，帐户配置为在系统上具有较少用户权限的用户受到的影响较小。 安全更新通过更正 Outlook 如何处理内存中的对象来解决该漏洞。		Outlook 2013 Outlook 2010
CVE-2020-1495	**Microsoft Excel 远程代码执行漏洞** 当 Microsoft Excel 软件未能正确处理内存中的对象时，该软件存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在当前用户的上下文中运行任意代码。如果当前用户使用管理用户权限登录，攻击者可以控制受影响的系统。然后，攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。与使用管理用户权限操作的用户相比，帐户配置为在系统上具有较少用户权限的用户受到的影响较小。 安全更新通过更正 Microsoft Excel 如何处理内存中的对象来解决该漏洞。	重要 远程执行代码	Office 2010/2013/2016/2019 365 Apps Enterprise Excel 2010/2013/2016 SharePoint EnterpriseServer 2013 SharePoint Server 2010 Office Online Server Office 2016/2019 for Mac
CVE-2020-1499	**Microsoft SharePoint 欺骗漏洞** 当 Microsoft SharePoint Server 未能正确过滤对受影响的 SharePoint 服务器构建的 web 请求时，存在欺骗漏洞。经过身份验证的攻击者可以通过向受影响的 SharePoint 服务器发送巧尽心思构建的请求来利用此漏洞进行攻击。 成功利用此漏洞的攻击者可以在受影响的系统上执行跨站点脚本攻击，并在当前用户的安全上下文中运行脚本。这些攻击可能使攻击者能够读取未经授权的内容，使用受害者的身份代表用户在 SharePoint 网站上执行操作，如更改权限和删除内容，并将恶意内容注入用户的浏览器中。 安全更新通过帮助确保 SharePoint Server 正确清理 web 请求来解决该漏洞。	重要 欺骗	SharePoint Server 2019 SharePoint EnterpriseServer 2016 SharePoint EnterpriseServer 2013 SharePoint Foundation-2010 SharePoint Foundation-2013

参考链接：

https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Aug
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV990001

➢ Apache Airflow 远程代码执行漏洞

发布日期：2020-08-4
更新日期：2020-08-4
受影响系统：
Apache Apache Airflow <=1.10.10
描述：

CVE(CAN) ID: CVE-2020-11982
Apache Airflow 是美国阿帕奇（Apache）软件基金会的一套用于创建、管理和监控工作流程的开源平台。该平台具有可扩展和动态监控等特点。
Apache Airflow 1.10.10 及之前版本中存在安全漏洞。该漏洞源于外部输入数据构造代码段的过程中，网络系统或产品未能正确过滤其中的特殊元素。攻击者可利用该漏洞借助恶意的 payload 执行代码。
建议：

厂商补丁：
Apache
厂商已发布了漏洞修复程序，请及时关注更新：
https://lists.apache.org/thread.html/r7255cf0be3566f23a768e2a04b40fb09e52fcd1872695428ba9afe91%40%3Cusers.airflow.apache.org%3E

➢ IBM UrbanCode Deploy 代码问题漏洞

发布日期：2020-08-9
更新日期：2020-08-9
受影响系统：
IBM UrbanCode Deploy 7.0.3.0
IBM UrbanCode Deploy 7.0.4.0
IBM UrbanCode Deploy 6.2.7.3
IBM UrbanCode Deploy 6.2.7.4
描述：

CVE(CAN) ID: CVE-2020-4481
IBM UrbanCode Deploy（UCD）是美国 IBM 公司的一套应用自动化部署工具。该工具基于一个应用部署自动化管理信息模型，并通过远程代理技术，实现对复杂应用在不同环境下的自动化部署等。
IBM UCD 中存在代码问题漏洞。远程攻击者可利用该漏洞获取敏感信息或消耗内存资源
建议：

厂商补丁：
IBM
厂商已发布了漏洞修复程序，请及时关注更新：

https://www.ibm.com/support/pages/node/6256128

➢ Zoho ManageEngine Desktop Central 整数溢出漏洞

发布日期：2020-08-04
更新日期：2020-08-04
受影响系统：
ZOHO ManageEngine Desktop Central <10.0.533
描述：

CVE(CAN) ID: CVE-2020-15588
Zoho ManageEngine Desktop Central 是集成的桌面和移动设备管理软件，可帮助从中央位置管理服务器、笔记本电脑、台式机、智能手机及平板电脑。
Zoho ManageEngine Desktop Central 10.0.533 之前版本的客户端存在整数溢出漏洞。攻击者可通过其控制的服务器通过特制 header 值利用该漏洞导致整数溢出。
建议：

厂商补丁：
ZOHO
厂商已发布了漏洞修复程序，请及时关注更新：
https://www.manageengine.com/products/desktop-central/integer-overflow-vulnerability.html

六、本期网络安全事件

➢ 装修公司花 240 万买 70 万条业主信息，5 市房管系统遭黑客入侵

2020 年 7 月 31 日据报道，2019 年，四川德昌县公安局破获一起公安部督办的“侵犯公民个人信息、黑客案”，侦破侵犯公民个人信息案件 20 件、非法获取计算机信息系统数据案 4 件，行政处罚多家涉案楼盘及其他相关公司，抓获犯罪嫌疑人 36 人。据警方调查，四川某装修公司为谋求快速发展，花费 240 余万元购买涉及川、渝、黔 3 省份近千楼盘 70 余万条公民个人信息。此案中，还有 4 人入侵四川 5 市房管系统，非法获取楼盘业主信息。

2020 年 7 月 30 日，记者从德昌警方获悉，截至今年 7 月 1 日，法院依法判决 27 人，还有多人被行政处罚，扣押、罚没涉案资金达 200 万元。目前，多家楼盘被行政处罚。针对所涉 5 市房管局，德昌警方已将相关线索通报 5 市网安部门。梳理发现，2018 年、2019 年，四川多地楼盘销售人员利用工作之便，将已售房屋的客户交易信息卖给该装修公司相关人员，一条信息价格为 3 至 5 元不等。该公司市场部人员进行电话诱导营销，迅速抢占装修市场。截至目前，该公司全体涉案人员均已落网。涉案的黑客马某某、杨某某等人也已被判刑。

『案发』装修公司花 240 万元购买近千楼盘 70 余万条信息

时间回到 2019 年 3 月 30 日，德昌县公安局收到四川某装修公司在德昌县某酒店召开装修推介会的线索，参会客户在事前均未向该公司提供过任何个人信息及联系方式。德昌县公安局随即派出卧底，发现该公司涉嫌非法持有公民个人信息，遂果断进行现场打击处理，并于当天直捣该公司总部。

据警方介绍，2015 年成立的该装饰设计工程有限公司，为谋求公司快速发展，花费 240 余万元购买川、渝、黔 3 省份近千楼盘 70 余万条公民个人信息。案发后，警方通过调取自 2015 年年底至 2019 年年初犯罪嫌疑人的通话清单，掌握了该公司重要的犯罪证据。2019 年 3 月 30 日，警方在案发地四川德昌抓获该公司法定代表人陈某某等人，公司直接负责购买信息的犯罪嫌疑人苟某某在逃，被广州警方抓获后拒不如实交代。在 2 名重要犯罪嫌疑人拒不交代的情况下，德昌警方通过缜密侦查，层层突破，最终关联出 30 余名贩卖信息的“串串”及楼盘公司“内鬼”，迅速查出所有人员的真实身份信息，最终通过集中式分批次收网，所有涉案人员全部归案。

『深查』警方抓获幕后黑客 四川 5 市房管局系统遭入侵

经深入侦查，该装饰设计工程有限公司的信息源头，除了公司自行找到楼盘业务员(内鬼)购买，多来自“串串”及黑客。经对犯罪嫌疑人的落地查证，德昌县公安局 3·30 侵犯公民个人信息专案组抓获达州籍黑客杨某某、南充籍黑客马某某。查实 4 人利用工作之便和网络技能入侵四川 5 市房管系统，非法获取楼盘业主信息。

经查，该装饰工程有限公司法定代表人陈某某及管理人员杨某某为走捷径拉拢客户，以占领装修市场先机和份额，高薪聘请专门从事购买公民信息的苟某某、郭某某开拓市场资源，发展业务，并授意财务主管王某负责与苟、郭二人具体对接操作，后又由王某将高价买回的业主信息分发给公司市场部进行电话诱导营销。截至目前，该装饰公司全体涉案人员已被一网打尽。

『进展』4 家楼盘被行政处罚 线索通报给 5 市网安部门

记者了解到，该案的破获，斩断了一条涉及川、渝、黔的全链条贩卖公民个人信息灰黑网络。据警方介绍，3·30 专案组在获得四川省公安厅批复的案件指定管辖决定后，全网打击处理涉及省内各地的非法获取、贩卖公民个人信息犯罪人员。截至目前，共立侵犯公民个人信息案 20 件，打处 30 余人，查处黑客入侵案 4 件、打处犯罪嫌疑人 4 人。

目前，德昌县 4 家楼盘因公司网络安全、信息安全意识淡薄，相关机制、规定不健全，保密安全等教育培训不到位，致公司不法员工有机可乘，将业主个人信息卖出，被德昌县公安局依法作出相应的行政处罚。德昌警方表示，针对本案所涉及的 5 市房管局，因网络安全

意识淡薄，网络安全管理主责未落实到位，德昌县公安局已将相关线索通报 5 市网安部门，将按照“一案双查”工作机制，依法追究未落实网络安全管理、信息系统保护主责的 5 市房管局。（来源：成都商报）

➢ 交行招行分别被罚 100 万：对客户个人信息未尽安全保护义务

2020 年 8 月 5 日，上海银保监局披露的两张罚单显示，交通银行股份有限公司太平洋信用卡中心和招商银行股份有限公司信用卡中心分别被罚 100 万元，违规案由涉及客户个人信息保护、催收、资信调查等。

具体来看，在交行方面，2019 年 6 月，交通银行太平洋信用卡中心对某客户个人信息未尽安全保护义务；2019 年 5 月、7 月，该中心对部分信用卡催收外包管理严重不审慎。招商银行信用卡中心在 2019 年 7 月对某客户个人信息未尽安全保护义务。此外，2014 年 12 月至 2019 年 5 月，该中心对某信用卡申请人资信水平调查严重不审慎。

上海银保监局责令上述两家银行信用卡中心改正，并分别处罚款 100 万元。

值得注意的是，有关银行客户个人信息保护的问题在今年上半年曾多次引发公众广泛关注。其中，一次是今年 4 月，疑似百万条银行保险机构客户数据被售卖；一次则是今年 5 月，脱口秀演员池子（王越池）发微博称，中信银行未获本人授权，便将他的个人账户流水提供给上海笑果文化传媒有限公司。

银保监会副主席黄洪在 4 月 22 日举办的国新办新闻发布会上表示，针对近期出现的银

行保险机构客户信息被贩卖一事，银保监会立即进行了全面排查，随后相关机构也陆续发表澄清声明。经查，在网上流传的被贩卖的客户信息绝大部分是黑客伪造或拼凑的。

在池子发微博直指中信银行未获本人授权将他个人账户流水提供给上海笑果文化传媒有限公司后，中信银行深夜回应此事并致歉，称该行已按制度规定对相关员工予以处分，并对支行行长予以撤职。

5 月 9 日，银保监会发布《关于中信银行侵害消费者合法权益的通报》，通报称，2020 年 3 月，中信银行在未经客户本人授权的情况下，向第三方提供个人银行账户交易明细，违背为存款人保密的原则，涉嫌违反《中华人民共和国商业银行法》和银保监会关于个人信息保护的监管规定，严重侵害消费者信息安全权，损害了消费者合法权益。银保监会消费者权益保护局表示，将按照相关法律法规，启动立案调查程序，严格依法依规进行查处。（来源：澎湃新闻）

➢ 一家名为 Anomaly Six 的美国企业向政府倒卖手机用户信息

2020 年 8 月 10 日报道指出，一家名为 Anomaly Six 的美国企业将自身软件开发包嵌入众多手机应用程序之中，进而追踪全球数亿部手机的位置信息。同时，该企业在用户不知情的情况下，将获取的这些信息转卖给了美国政府。

法庭记录和该报进行的采访显示，Anomaly Six 由两名承接国防合同的退伍军人创建，其职业生涯大部分时间都与美国政府机构密切合作。营销材料显示，**该企业能够从超过 500**

款手机应用程序中获得用户的位置数据，其中部分是通过将其软件开发包植入手机应用程序实现的。

报道称，手机应用程序开发者通常允许第三方公司将软件开发包植入自身程序，目的是为了赚取一定费用，而这些第三方公司转而又通过出售从应用中获得的数据来谋利。用户很难知道应用程序中是否植入了此类软件开发包，因为大多数隐私政策都不会披露这些信息。在对许多业内人士进行采访后指出，当前美国几乎没有限制此类交易的监管规定。

报道强调，尽管目前在美国广告、市场营销等行业，许多私营企业都从事买卖位置数据的交易，但与美国国家安全机构有密切联系的企业直接收集用户位置数据，是极不寻常的。该报还发现，Anomaly Six 提供的服务与另一家名为 Babel Street 的公司类似，后者为美国情报和执法机构提供社交媒体监控服务。Babel Street 一款名为 Locate X 的产品，也为客户提供从用户应用程序中提取的手机位置信息。事实上，Anomaly Six 的创始人之前都在 Babel Street 任职，负责该公司与美国国防部、司法部、美军网络司令部以及情报机构的关系。

报道指出，根据法庭记录，Locate X 在设计时就采纳了美国政府官员的部分意见，开发后则被美国军事情报部门广泛使用。美国联邦合同数据显示，Babel Street 还与美国国土安全部、司法部等机构签订了合同。报道称，被收集的手机位置信息可用于“生活模式”分析，帮助理解、预测情报目标的习惯和行为。

美国乔治城大学法学教授劳拉·梅表示：“用户并不知道的是，当他们安装天气应用程序、游戏程序或任何其他看似无害的应用程序时，自己的私人位置数据将被收集和出售。很明显，这就是正在发生的事，这种做法没有透明度。”（来源：人民日报）

➢ 澳洲大学在线考试系统遭黑客攻击，数十万用户数据被泄露

2020 年 8 月 6 日据澳媒报道，澳洲有关部门正在调查澳洲大学正在使用的一个在线考试工具的数据安全隐患。悉尼大学的一位发言人表示，该校周四与 ProctorU 公司进行了会面，并确认正在对一起机密数据泄露事件进行调查。

“任何这种类型的安全和隐私泄露事件令人深感担忧，我们将继续与 ProctorU 合作，了解泄露事件的相关情况，并确定是否需要采取任何后续行动。我们还将评估今年在线考试和监考的经验，为我们在 2021 年的学业评估方法提供参考。我们今天会见了 ProctorU 的首席执行官和合规官员，他们证实目前正在调查一起与服务用户相关的机密数据泄露事件，”

该发言人说道。

这名发言人表示：据悉尼大学了解，这些泄露的数据与 2014 年或之前注册为 ProctorU 用户的人有关。“我们认为学校现有在校学生没有受到这次泄露事件的直接影响，因为我们在 2020 年才开始使用 ProctorU 的在线代理服务，以应对新冠大流行。”

在冠状病毒大流行造成“封锁”后，澳洲各地的大学迅速将学习和学业评估转移到了线上，使用 ProctorU 来监督在线考试。悉尼大学学生报 Honi Soit 报道了这起数据泄露事件，并表示这也影响到了其他大学。报道称，此前学生对大学使用该服务提出了严厉批评，认为 ProctorU 侵犯了学生的隐私。

ProctorU 允许监考员在学生在线考试时，通过电脑摄像头监督学生。

Honi Soit 报道称，黑客公布了一个包含数十万 ProctorU 用户记录的数据库，其中包括属于悉尼大学工作人员的记录。这些数据包括姓名和地址、用户名和未加密的密码。新南威尔士大学的一位发言人表示，该校已被告知“被泄露的数据库中不包含与新南威尔士大学有关的记录”，因此该校的数据不受影响。

在 Honi Soit 文章中被点名的 James Cook University 表示，该校没有使用 ProctorU 服务。使用了 ProctorU 服务的昆士兰大学表示，该校的安全问题没有受到影响。（来源：腾讯新闻）

➢ 利用“抓包软件” 抓走 14 万 七名年轻人被判盗窃罪

2020 年 7 月 29 日，据厦门晚报报道：偶然得知一款应用程序有漏洞，可从中提现获利，小伙子忍不住尝试了一把。看着几千元入账，仿佛天上掉馅饼，他又找来表哥、同学、网友一起干。最终，这 7 名年轻人都背上了盗窃的罪名。近日，湖里区法院审理了一起特殊的盗窃案。这起盗窃案有 7 名被告人，年纪最大的 25 岁，最小的只有 19 岁。被告人孙某 20 岁，来自河南，作案前刚通过成人高考。2019 年 6 月 24 日，孙某从一名网友那里得知，一款具有支付功能的社交应用程序存在提现方面的漏洞，可以通过“抓包软件”提现转至银行卡。孙某心动了，当天上午 8 点，他注册了账户，绑定了银行卡，成功进行提现操作，盗得 6439 元。

接着，他开始向身边的人搜集手机号码、银行账户等信息，在应用程序上注册更多账号，并向他人许诺“分成”。孙某用其表哥王某的银行卡提现得到近 1.4 万元，自己从中分得 9000 元，剩余的钱给了表哥。此外，他还找了几名同学、网友参与进来，有的甚至还介绍同学加入。最多的一笔提现 2 万多元。就这样，仅用了五六个小时，孙某就从该应用程序上盗窃逾 14 万元。

2019 年 9 月 12 日，孙某和表哥王某主动向公安机关投案。之后，孙某协助公安机关，

劝说其他被告人自首。直到 2019 年 12 月，7 人均归案，并向受害单位退赔了经济损失，取得谅解。

湖里区法院一审认为，孙某等人以非法占有为目的，窃取他人财物，构成了盗窃罪。其中孙某参与盗得 142167.5 元，数额巨大，而且孙某在共同犯罪中起主要作用。考虑到孙某是自首，并协助公安机关抓捕其他被告人，有立功表现，可以从轻处罚。湖里区法院一审判处孙某有期徒刑 2 年 6 个月，缓刑 3 年，并处罚金 3 万元，其余 6 名被告人也均适用缓刑，并处罚金。

【法官提醒】面对屏幕不要心存侥幸 只要一伸手就别想逃脱：在湖里区法院刑事审判庭，利用网络漏洞，采用“抓包软件”盗窃的刑事案件已不是首例。负责审理孙某一案的法官告诉记者:“审理过几件，作案的都是年轻人。”据她的观察，这些年轻人喜欢研究黑客技术，在互联网上组建交流群。在现实生活中，这些年轻人不会去做偷、抢这种违法的事，但是在网络上，面对电脑屏幕、手机屏幕就心存侥幸，没有意识到自己的行为严重违法。这名法官介绍，她曾经审理过另外一起案件，未成年的被告人利用“抓包软件”，仅充值 1 元，然后操作提现、篡改数据，瞬间非法获利 30 万元。案件审理时，考虑其认罪悔罪的表现等因素，进行了从轻处罚。可是后来，这个被告人还是再犯了。“他们觉得来钱太快，觉得可能不会被查到，但其实只要一伸手，就别想要逃脱。”

【名词解释】抓包：“抓包”就是将网络传输发送与接收的数据包进行截获、重发、编辑、转存等操作。而“抓包软件”就是拦截查看网络数据包内容的软件。（来源：厦门晚报）

➢ 第一弹 App 负责人被批捕 上传盗版非法获利 3418 万余元

2020 年 8 月 12 日，中国打击侵权假冒工作网发布一起盗版影视 APP 侵犯著作权案。据悉，近日，静安区检察院对 22 名通过盗版影视 APP 播放侵权视频的犯罪嫌疑人批准逮捕。其中，16 名犯罪嫌疑人以涉嫌侵犯著作权罪批捕，6 名犯罪嫌疑人以涉嫌侵犯著作权罪、帮助信息网络犯罪活动罪双罪名批捕。

经查，自 2019 年开始，上海斯干网络科技有限公司在未经著作权人许可的情况下，以第一弹 APP 为平台，擅自上传大量美国、日本、韩国等国家的影视剧集，从中收取会员充值费及广告费用。同时，斯干公司为解决片源下载问题，专门成立安徽红岸科技有限公司，负责第一弹 APP 的影视剧集审核及下载上传工作。经司法审计鉴定初审，斯干公司通

过第一弹 APP 发布侵权视频 2 万余集，收取会员费 992 万余元，收取广告费 2426 万余元，合计非法获利 3418 万余元。

由于本案涉案犯罪嫌疑人众多，侵权视频数量巨大且涉及向国外版权方取证等多重困难，为确保办案质量，部门提前介入案件，听取公安机关汇报案情和侦查进度，引导侦查取证。受案后，部门六名检察官加紧审查，完成了对 35 名涉案犯罪嫌疑人的提审、证据补充、审结报告制作等任务，并多次向分管检察长汇报案件审查情况，确保了审查逮捕阶段的办案质量。（来源：静安区双打办）

信息安全意识产品服务

021-33663299