国盟信息安全通报

2020 年 5 月 24 日第 216 期

全国售后服务中心

国盟信息安全通报

（第 216 期）

国际信息安全学习联盟

2020 年 05 月 24 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 336 个，其中高危漏洞 115 个、中危漏洞 199 个、低危漏洞 22 个。漏洞平均分值为 6.16。本周收录的漏洞中，涉及 0day 漏洞 154 个（占 46%），其中互联网上出现“Zyxel NBG-418N v2 Modem 跨站请求伪造漏洞、Joomla!组件 prayercenter 'id' SQL 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 7595 个，与上周（5514 个）环比增加 38%。

主要内容

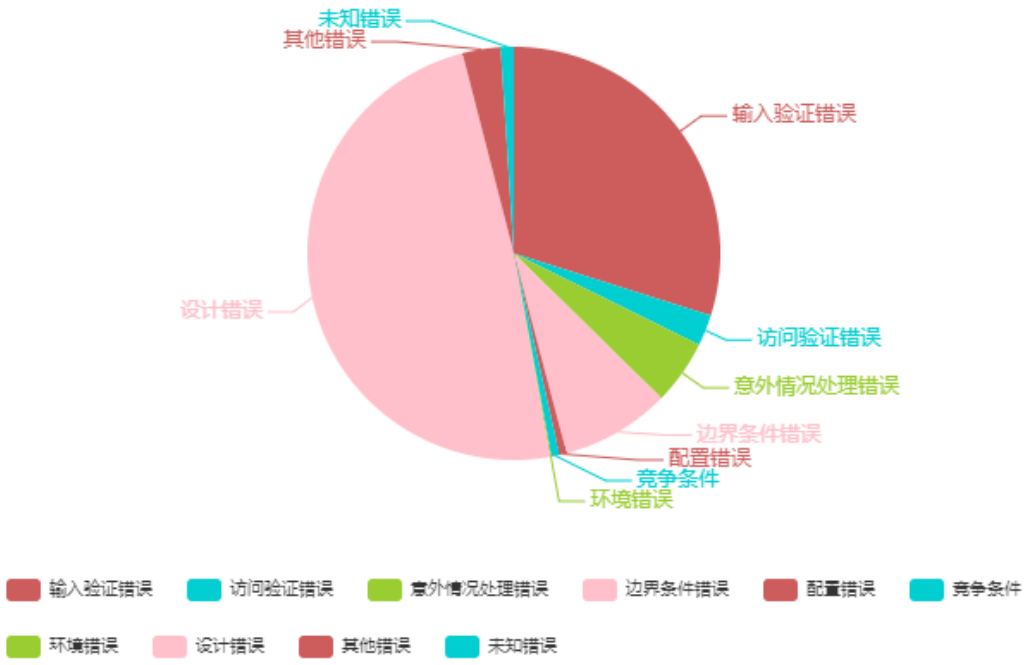
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

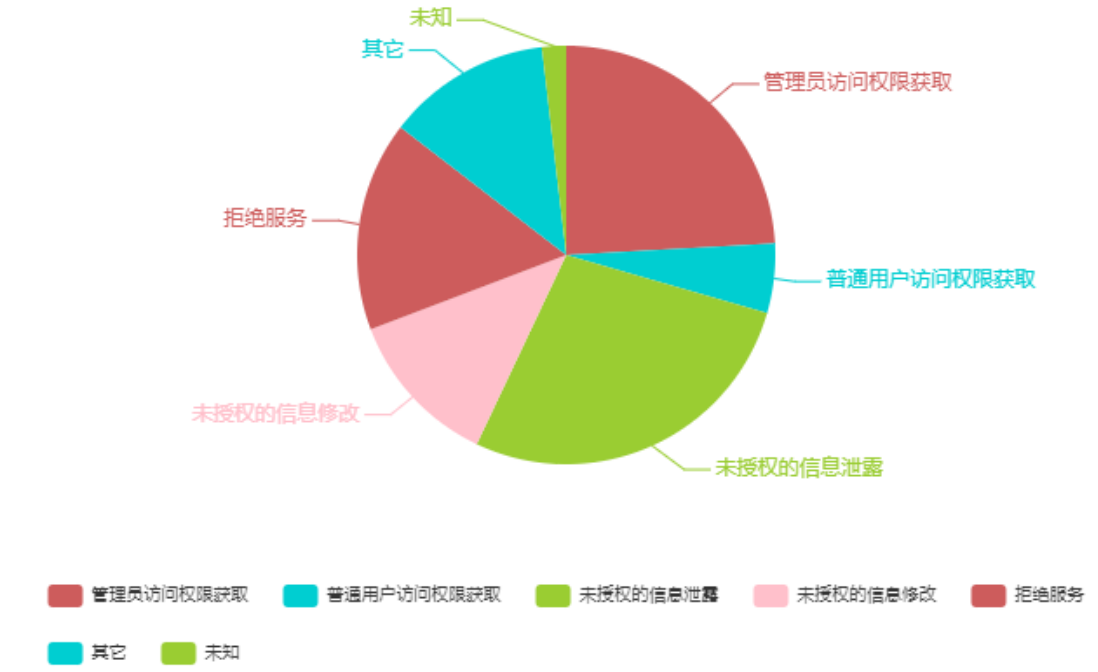
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 336 个，其中高危漏洞 115 个、中危漏洞 199 个、低危漏洞 22 个。漏洞平均分值为 6.16。本周收录的漏洞中，涉及 0day 漏洞 154 个（占 46%），其中互联网上出现“Zyxel NBG-418N v2 Modem 跨站请求伪造漏洞、Joomla!组件 prayercenter 'id' SQL 注入漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 7595 个，与上周（5514 个）环比增加 38%。

二、安全漏洞增长数量及种类分布情况

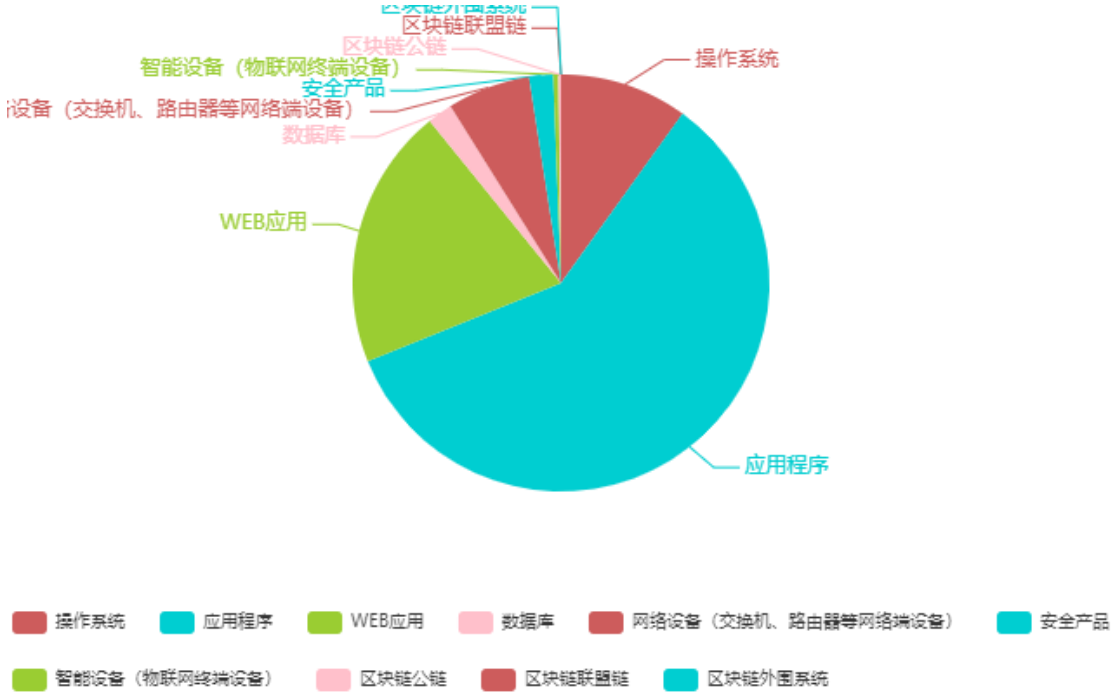
➢ 漏洞产生原因（2020 年 05 月 10 日—2020 年 05 月 24）



➢ 漏洞引发的威胁（2020 年 05 月 10 日—2020 年 05 月 24）



➢ 漏洞影响对象类型（2020 年 05 月 10 日—2020 年 05 月 24）



三、安全产业动态

➢ 全国两会代表委员网络安全提案内容

十三届全国人大三次会议、全国政协十三届三次会议分别于 5 月 22 日、5 月 21 日在京召开。今年全国两会“非同寻常”，不仅因为“非常”的会议时间，更因“非常”的历史节点。本文根据国家互联网信息办公室公布，互联网、整理了全国两会代表委员对于网络安全提案内容。

周鸿祎：着眼“新基建、5G、工业互联网、信创网络安全”

今年两会，周鸿祎提交了四份提案，全都紧密围绕网络安全展开。四份提案分别建言：

1、尽早构建新基建网络安全防护体系

今年以来，国家层面屡次提及“新基建”。4 月 29 日，中共中央政治局常务委员会强调，要启动一批重大项目，加快传统基础设施和 5G、人工智能等新型基础设施建设。周鸿祎认为，国家推动新基建，是很有前瞻性与魄力的决策，相当于我们又有机会比其他国家领先一步，尽快实现全社会、全行业数字化。但随着新基建进一步促进网络空间与物理空间的连通和融合，加快了“大安全”时代的来临。网络安全不再只影响虚拟空间，而是扩展到了现实世界，对国家安全、社会安全、人身安全造成严重影响。

因此，对于构建新基建网络安全防护体系，提出 4 点建议：

- 运用整体思维，规划新基建网络安全防护体系顶层设计；
- 同步建设新基建的安全基础设施，聚焦新基建安全防能力构建；
- 强化大数据平台安全，实现安全的大数据协同计算；
- 开展常态化网络安全攻防对抗演习持续检验和提升新基建安全能力。

2、尽快制定《国家 5G 安全战略》

作为新一代的数字基础设施，5G 在赋能发展的同时也将引发新的网络安全风险，其安全性具有基础性和全局性意义。今年 3 月，工信部发布《关于推动 5G 加快发展的通知》也明确表示，着力构建 5G 安全保障体系。因此，周鸿祎建议，应当从战略高度审视 5G 网络安全的重大意义和紧迫性，加强 5G 安全的顶层设计，制定《国家 5G 安全战略》。

3、加快推进工业互联网安全保障

周鸿祎认为，“工业互联网是新基建最大的应用场景之一”，保障新基建安全应重点“盯防”工业互联网的安全。对此，他建言加快推进工业互联网安全保障建设，为国家实体经济和社会保驾护航。

4、加强信创网络安全保障能力建设。

信息技术创新应用作为我国信息技术领域打造自主创新生态的国家战略举措，也是新基建的重要抓手。在周鸿祎看来，未来 3 到 5 年，信创产品和解决方案将在更多领域规模化推广应用。其安全问题将面临前所未有的挑战，因此，他建议要强化信创安全体系顶层设计、统筹构建安全保障体系。

李彦宏：对疫情期间采集的个人信息设立退出机制

李彦宏同样提交了四份提案，包括个人信息保护、构建人工智能新型基础设施、加快智能交通基础设施建设和鼓励继续教育。

可以发现，其中 2 份提案都与疫情直接相关，尤其是关于加强对疫情防控相关个人信息保护的提案。李彦宏建议相关部门统筹联动、做好对疫情相关个人信息的管理以及疫情后的信息处置工作。

针对新冠肺炎疫情期间：

1、采集的个人信息设立退出机制。

2、加强对已收集数据的规范性管理，最大限度地降低数据泄露、滥用风险。

3、研究制定特殊时期的公民个人信息收集、存储和使用的标准和规范。

马化腾：加快推进产业互联网建设的举措与建议

马化腾是两会的常客，连续八年提交多达 40 余份建议，但今年因身体原因请假，缺席两会。继去年两会在产业互联网领域提交建议并获国家部委答复后，马化腾今年进一步提出《关于加快制定产业互联网国家战略 壮大数字经济的建议》。

其中，提出了六项加快推进产业互联网建设的举措和建议：包括加强顶层设计，制定系统推进产业互联网发展的国家战略；加快推进云计算等新基建，筑牢数字经济发展的战略基石；以“数据中台”建设为重点和突破口，进一步推动数据开放共享，提高数字化治理水平；持续推进开源协同创新生态，打造产业互联网“朋友圈”，提升科研创新数字化水平，同时加大产业安全投入。

此外，更完善的网络信息安全体系是数字经济的高质量发展的基础，马化腾建议，要加大安全人才培养、核心技术突破、安全生态协同，充分发挥网络信息安全在数字经济建设中的核心保障价值，建设以产业为中心的、原生的、主动规划为特征的新型“产业安全”体系。

张野：新基建为网络安全产业带来机遇

张野今年带来的 3 个提案之一是“提高我国网络安全应急处置能力”。由于我国网络安全基础薄弱，导致了网络攻击猖獗，难以实现有效的持续监控，供应链受制于人，网络安全信息收集、研判仍然分散，时效性较差，网络安全事件处置中资源协调调配效率较低，亟需对现有网络安全建设成果进行整合、统筹利用，建立统一的指挥调度系统，构建有效的网络安全防护处置体系，形成快速处置反应能力和网络威慑能力。

具体的研究建设中，张野认为，网络安全事件的发生具有传播快、影响范围广、需分析溯源等特点，在很多方面可以借鉴传染疾病的防控措施和手段。由于我国在公共安全领域的应急体系建设已经比较完备，《国家物资储备管理规定》等相关法律规章对物资储备、使用等也有明确的规定，因此，配套制定网络安全处置应急征用办法可以借鉴我国在公共安全领域的应急体系，特别是医疗卫生应急体系的建设经验。

肖新光：建立完善战备级的网络安全应急和资源储备机制

再过去两年里，肖新光的提案分别为《在网络空间安全领域进行针对性投入和布局应对重大地缘安全风险的提案》、《关于通过系统规划指引、保障资源投入、加强问责落实，全面提升政府央企网络防护水平的提案》，他认为：“网络安全防控能力薄弱，难以有效应对国家级、有组织的高强度网络攻击”是众多风险中的一项突出风险。而今年的提案延续以往的大主题，并且结合疫情时事。肖新光指出，突发的疫情带来了网络安全次生风险，暴露了系列安全隐患。为此，他的提案围绕建立完善战备级的网络安全应急和资源储备机制，来应对重大的突发性综合风险。

严望佳：安全建设智慧城市

在严望佳看来，当前在建设智慧城市过程中，容易忽视的网络安全问题有以下几方面：

1、缺乏智慧城市网络安全监管责任主体；

2、智慧城市与信息安全发展关系亟须正确对待；

3、智慧城市存在重大数据安全风险；

4、智慧城市大量使用物联网技术存在安全风险；

5、智慧城市关键技术存在失控风险。

针对这些问题，严望佳提出了切实可行的 6 点建议：转变智慧城市安全建设思想，由同步建设转为安全先行；转变智慧城市安全建设思想，由同步建设转为安全先行；正确处理智慧城市与信息安全发展关系；确保智慧城市数据安全保护；制定物联网安全技术方向鼓励智慧城市关键技术引进和创新。

杨元庆：5G+工业互联网的现实挑战

杨元庆向十三届全国人大三次会议提交包括围绕建设新一代互联网医疗健康平台、推动信息产品消费、推动新基建和智慧经济建设、推动制造业高质量发展等领域的多份建议。

围绕新基建相关的“5G+工业互联网”，他提到了在制造业仍面临的一些难点和挑战。

一是数字基础设施建设迫在眉睫。新全国性的新冠疫情催生了如生产数字化、在线办公、无人物流等互联互通需求，但在实际应用中，暴露出企业数字化程度不均、工厂设备联网率有待提升等问题。

二是工业信息安全问题比较突出。近年来，针对工控系统的网络攻击、网络入侵等安全事件频发。在无线、5G 时代，存在“端-边-云-网-智”的系统化安全问题，涉及工控、网络传输和数据安全等多方面，需要构建体系化的监管机制，否则很难为制造业全产业链抵御外部攻击。此外，目前还缺乏支持 5G 的专用工业设备、高速数据处理和分析的计算设备以及自主可控的工业软件平台，给行业应用也带来了一定安全隐患，需要加大技术研发和设备改造力度。

三是应用场景和盈利模式有待挖掘。

此外，5G 刚刚迈入商用，市场和投融资还处于起步阶段，结合 5G 新特性的移动化应用生态、运营支持、标准体系尚未成熟。

从目前的网络安全提案来看，来自企业的声音正在变得更加多元和丰富，围绕新基建、5G、疫情等话题开展的提案质量也在不断提高。（来源：互联网综合整理）

➢ 5G 时代的个人信息安全 GB/T35273-2020《个人信息安全规范》推介

4G 改变生活，5G 改变社会。2019 年被公认为 5G 元年，美国、韩国、英国等国家在 2019 年上半年，都先后启动 5G 商用。2019 年 10 月 31 日，中国三大电信运营商共同宣布 5G 商用并发布了 5G 套餐，至此 5G 正式走进了中国的千家万户。

作为“新基建”的重要组成部分，5G 在我国中国特色社会主义新时代的建设进程中，发挥着极为重要的作用。一方面，作为数字经济、中国制造 2025 的重要基础设施，5G 对于经济的拉动作用明显。根据中国信通院报告预测，2020 年至 2025 年期间，中国 5G 商用直接带动的经济总产出 10.6 万亿元，直接创造的经济增加值 3.3 万亿元。另一方面，5G 开启的万物互联时代，对于社会的运行和治理亦将产生深远影响。以 2020 年初抗击新冠疫情为例，5G 与人工智能、大数据等技术广泛融合，在防控筛查、民生保障、医学治疗、复工复产等方面都发挥了重要作用，人们也逐步开始接受并使用如体温监测、远程医疗、在线教学等 5G 服务。

未来，伴随着 5G 技术超高速率、超大连接、超低时延特性的进一步发挥与展现，以及 5G 对生产、生活、社会治理等领域的进一步赋能和渗透，可以预见全社会收集和掌握的数据，在种类、数量、颗粒度、实时性等维度方面也将会大幅提升，并不可避免地会涉及到更多个人信息，以至个人敏感信息。如何在 5G 时代合理合法合规运用数据，为各行各业高效赋能的同时保护好个人信息安全，成为了一个亟待解答的问题。2020 年 3 月 6 日，国家市场监督管理总局和国家标准化管理委员会发布 GB/T 35273-2020《信息安全技术 个人信息安全规范》（以下简称 2020 版《个人信息安全规范》），其在原有 GB/T 35273-2017 基础上进行更新，从个人信息安全基本原则、个人信息的收集、存储、使用、委托处理、共享、转

让、公开披露，以及个人信息主体的权利、个人信息安全事件处理、组织的个人信息安全管理要求等诸方面，对于个人信息安全进行了技术规范，并且增加了“用户画像的使用限制”、“基于不同业务目的所收集个人信息的汇聚融合” 等新章节内容。2020 版《个人信息安全规范》的提出，在很大程度上结合和适应了 5G 时代的新情景、新变化，给相关机构的个人信息安全管理提供了参考标准和架构。

一、5G 时代的个人信息特征

5G，即第五代移动通讯技术，根据 ITU 定义，将在峰值速率、用户体验速率、频谱效率、移动性、时延、连接密度、网络效能、流量密度八个维度进行显著提升。其中，从应用和体验角度，较为明显的变化是峰值速率（10 Gbits/s）、连接密度（106 设备/km2）和时延（1ms）。在具体的场景中，5G 将主要围绕增强型移动宽带（eMBB）、大规模机器通信（mMTC）、高可靠低时延通信（uRLLC）三个场景展开，并体现出个人信息的一些新特征。

在 eMBB 场景下，5G 将可以提供远超 4G 的超高带宽，预计典型应用为超高清视频、AR/VR、沉浸式教学或游戏、360 度全景直播等，涉及的个人信息更加广泛。以沉浸式教学为例，这种模式提供了一种虚拟学习环境，通过增强参与、互动、演练进而达到提升教学效果的目的。这种模式提供的服务，依赖于系统对受教者实时数据的分析、模拟、决策，教学过程中收集的教育记录、培训记录、浏览记录、使用记录等个人信息量相比传统教育模式有大幅增加。尤其是当涉及到一些特殊人群（如 14 岁以下儿童），或与人工智能、面部识别等新技术结合的情景，这一特征将变得更为突出，对于个人信息安全的需求和要求也更高。

在 mMTC 场景下，万物将实现互联，接入网络的个人设备不再限于手机、Pad、电脑，如智能手环等随身设备，以及智能门锁、智能安防等智能家居产品，将大量连入网络并传输数据。根据 GSMA 预测，2025 年世界将有 250 亿台设备接入 5G 网络并实现互连。这将给个人信息带来两个变化，一是个人信息将更加的碎片化，大量的设备都可能收集并传输一定量或某种程度的个人信息（个人敏感信息）并作为其提供服务的前提和基础，个人信息的管理将变得更为复杂；二是个人信息虽然碎片化，但是由于数据维度的增加、数据来源的增长， 个人信息整合、汇聚后的价值迅速提升，其在用户画像、个性化展示等应用上的作用更加突显，因此亟需加强规范和管理。

在 uRLLC 场景下，超低时延的通信成为现实，无人驾驶、远程医疗等需要高可靠、低时延网络支撑的应用将逐步实现。这一场景下的个人信息同样体现出了一些新特征。以无人驾驶为例，无论是 C-V2X，或是远程驾驶，都涉及到大量的位置信息，如果与特定主体的身份个人信息、设备信息（如 IMSI、IMEI）关联，很容易衍生为个人行踪信息等个人敏感信息。

同样，在远程医疗应用中，无论是远程会诊，或是远程遥控手术、超级救护车，大量的个人健康生理等高度敏感的个人信息通过网络进行传递，且这种数据传输近乎实时，因此其管理值得高度关注。

二、2020 版《个人信息安全规范》对 5G 的适用性

2020 版《个人信息安全规范》是在 GB/T 35273-2017 基础上的更新迭代，此次版本尤其结合了国际上部分国家和地区最新法律、法规（如欧盟《通用数据保护条例》（General Data Protection Regulation）），部分新技术典型应用场景（如基于人工智能、大数据的用户画像），以及当前个人信息安全遇到的突出问题，增加或修改了部分内容，整体上更具实用性和前瞻性。2020 版《个人信息安全规范》的相关内容，同时也体现了 5G 时代的个人信息特征，并具有较强适用性。

首先，2020 版《个人信息安全规范》对于个人信息的全生命周期管理进行了规范，从个人信息的收集、存储、使用、委托处理、共享、转让、公开披露等关键环节，均进行了技术规范，并且从个人信息处理者的角度，对于个人信息安全事件处理、组织的个人信息安全管理提出了要求。5G 赋能千行百业，未来在 5G 技术的支持下，无论是传统行业的数字化转型，或是新行业新模式的创新发展，都必然会导致有越来越多的企业开始关注、收集、运用数据核心资产，对于个人信息安全和保护的需求也将大幅提升。在这方面，2020 版《个人信息安全规范》虽属于推荐标准，但其涵盖内容相对完整，并体现出针对中国境内个人信息安全的特点，具备较强的参考意义。

其次，2020 版《个人信息安全规范》契合了 5G 时代个人信息的新特征，并作出规范。例如，针对 5G 时代 mMTC 场景下，愈来愈多的设备具备采集、传输、处理数据和个人信息能力，个人信息呈现碎片化，但整合利用价值巨大的特点，2020 版《个人信息安全规范》在 7.6 节增加了“基于不同业务目的所收集个人信息的汇聚融合”内容，从使用目的限制，汇聚后开展个人信息安全影响评估，采取有效的个 人信息保护措施等实际动作方面进行了规范。这对于 5G 时代，通过汇聚整合万物互联情景下不同渠道收集的数据，尝试创新的商业模式， 在合规和操作方面非常具有意义。

同样，2020 版《个人信息安全规范》在 9.7 节中，增加了对于第三方接入管理的章节内容，从个人信息控制者角度，对于不属于委托处理、共同个人信息控制者情形下的具备收集个人信息功能的第三方产品或服务的管理，进行了规范和要求。相关内容适应了 5G 时代

uRLLC 场景下的无人驾驶、远程医疗等应用中需要多方协同的情形。随着 5G 技术带来

超高速率、超大连接、超低时延通信的实现，以及智慧城市等平台类应用的快速发展，未来以 5G 为基础的商业模式将更趋多元化，形态更趋丰富和多样化，因此更需要多方的合作与协作。其在处理个人信息和数据的过程中，也会更多涉及到诸如 SDK、小程序、软件开发包等第三方产品和服务，而这也恰恰是当前个人信息安全的一个薄弱环节和风险点。2020 版《个人信息安全规范》在此次版本更新中，特别对这一情形进行了界定，对个人信息控制者提出了涵盖安全评估、合同责任明示、向用户明确标识、记录留存、第三方响应机制等诸多内容的规范要求，具有很强的针对性。

三、5G 技术对个人信息安全的支撑作用

5G 作为一种网络信息技术，其具备一些独特属性，也具备有效支撑个人信息安全的能力和潜力。

1、网络切片技术

网络切片是 5G 网络的特征之一。5G 时代，在统一网络基础设施架构下，电信运营商可通过采用硬切、软切等多种方式，将 5G 网络划分为不同的切片。划分出的若干网络切片，可以实现性能上的差异化，即同一基础网络可以同时满足不同业务对 SLA、速率等网络属性的异质化要求，并可根据用户需求进一步实现网络隔离、敏捷部署、独立运营、弹性网络等功能。基于切片技术的网络隔离、独立运营等属性，可以很好适应部分个人信息（尤其是个人敏感信息）传输过程中的特别需求。例如，在远程医疗应用中，会涉及大量的个人健康生理信息和数据传输，并且对网络时延、速率、稳定性、网络安全性有很高的要求，则可考虑采用网络切片技术进行支撑，确保其中的个人信息安全。

2、边缘计算技术

5G 时代随着如自动驾驶等低时延、高可靠应用的快速发展，对于近终端的计算需求不断增长，相关的个人信息安全保护也变得愈加重要。在“云管端”的基础上，边缘计算以其对实时分析和决策的有力支撑，获得了较多关注。5G 可以非常好的与边缘计算融合、协同。通过在接入网、汇聚网等层面的部分单元部署边缘计算节点的方式， 可以在降低时延、提升下行吞吐量的基础上，减少非必要个人信息的传输或存储，实现隔离，进而保障个人信息安全。

综上所述，5G 技术带来的通信能力提升，对于个人信息和个人信息安全而言，既是机遇亦是挑战。GB/T 35273-2020《信息安全技术个人信息安全规范》在很大程度上体现了 5G 个人信息特征，提出了有针对性的技术规范，适应了 5G 时代的个人信息安全需求。相信对于期望抓住 5G 机遇，创新发展的各类数字经济从业机构，都将具有非常好的指导意义。（来

源：全国信息安全标准化技术委员会网站）

➢ 《个人金融信息保护技术规范》热点问题分析

金融领域个人信息违法违规行政和刑事执法案例数量在 2019 年呈爆发式增长趋势，特别是 2019 年 9 月以来，刑事力量已经开始介入与金融行业密切相关的大数据行业。在此背景下，金融领域的个人信息保护立法备受关注。由于 2019 年的《中国人民银行金融消费者权益保护实施办法》（征求意见稿）和《个人金融信息（数据）保护试行办法》（征求意见稿）目前仍在征求意见之中，2020 年 2 月 13 日，经中国人民银行颁布并实施的《个人金融信息保护技术规范》（JR/T 0171-2020）（以下简称“《技术规范》”），引起各界热议。

一、《技术规范》的法律性质

《技术规范》发布以来，有人认为，该《技术规范》是中国人民银行颁布的规范性文件，具有一定的强制性；还有人认为，该《技术规范》只是一个行业推荐标准，并无强制性，那么，如何看待《技术规范》的法律性质呢？

《技术规范》其实是由全国金融标准化技术委员会（SAC/TC 180）（以下简称“金标委”）归口的金融行业推荐性标准，而金标委是国家标准化管理委员会授权，在金融领域内从事全国性标准化工作的非法人技术组织；之所以《技术规范》由中国人民银行发布，是因为中国人民银行受国家标准化管理委员会委托对金标委进行领导和管理。

尽管如此，《技术规范》由中国人民银行科技司提出并负责起草，其参考和引用了在业界非常有影响力的《个人信息安全规范》，而中国支付清算协会、中国互联网金融协会、银

联、网联、商业银行、支付机构、保险公司、证券公司、金融认证机构等多家单位，也共同参与了起草工作。

可以预见的是，中国人民银行今后关于金融领域的个人信息保护的立法工作，很有可能会参考甚至引用《技术规范》的相关内容。从这个意义上讲，我们建议在实务中将其理解为“准强制性标准”，并尽量以其作为合规风险的衡量准绳。

二、《技术规范》的适用范围

根据《技术规范》的有关规定，其适用于提供金融产品和服务的金融业机构，而根据其定义，“金融业机构是指由国家金融管理部门监督管理的持牌金融机构，以及涉及个人金融信息处理的相关机构”。我们注意到，不少作者对于涉及个人金融信息处理的相关机构做了扩大性的解释，认为金融产业链的相关机构均可能落入《技术规范》规制范围，其中包括助贷、P2P、贷后管理（如催收）等非持牌机构，甚至包括提供身份验证服务的电信服务商、信息技术提供商、风控服务解决方案提供商、市场营销服务提供商等。

我们认为，不宜对金融业机构做此类扩大解释。首先，《技术规范》虽然规定“金融业机构”包括“涉及个人金融信息处理的相关机构”，但是，根据《技术规范》的规定，“个人金融信息”是指“金融业机构通过提供金融产品和服务或者其他渠道获取、加工和保存的个人信息”，两相结合，难免有循环定义之嫌。其次，根据《中华人民共和国立法法》的有关规定，在没有明确的法律或行政法规等上位法律依据的情况下，有关规章规范的内容，不得设定减损公民、法人和其他组织权利或者增加其义务的内容。而《技术规范》作为行业的推荐性标准，其起草和制订也未见相关行业从业者参与其中，如将金融业机构做扩大性解释，显然也不合理。第三，之所以把《技术规范》视为“准强制标准”是由于日后的立法和监管执法可能会参照或者援引相关规定，除非能够给上述金融产业链的所有相关机构明确监管部门，否则，有关规定也无异于水中捞月，根本无法落地。

当然，不对适用范围做扩大性解释，并不意味着《技术规范》对于涉及金融行业产业链的相关机构没有任何影响。监管部门对于持牌金融机构或征信机构等受其监督管理机构的要求和执法，同样会让其将受到监管的合规压力向相关行业和机构进行传输，最后对整个行业造成巨大的影响。届时，有关机构出于业务的压力，可能也需参照《技术规范》的要求进行相应的调整。

三、《技术规范》中授权同意的例外

由于个人金融信息的特殊性，中国人民银行等金融监管部门一直关注个人金融信息的授权同意的要求。从 2005 年颁布的《个人信用信息基础数据库管理暂行办法》和 2011 年颁布

的《人民银行关于银行业金融机构做好个人金融信息保护工作的通知》，到 2013 年颁布的《征信业管理条例》和 2016 年颁布的《中国人民银行金融消费者权益保护实施办法》，再到 2019 年颁布的《中国人民银行金融消费者权益保护实施办法》（征求意见稿）和《个人金融信息（数据）保护试行办法》（征求意见稿），都对个人金融信息的采集和使用提出了严格的获取个人客户授权同意的要求。但是，上述法规基本没有考虑到取得授权同意的例外情形。

我们认为，个人金融信息由于具有人格属性和财产属性双重特点，同时，也对国民经济具有重要影响力，对于个人金融信息的采集、处理、使用进行严格要求，无可厚非。但是，目前我国关于个人金融信息的定义范围非常广泛，以 2016 年颁布的《中国人民银行金融消费者权益保护实施办法》为例，个人金融信息“是指金融机构通过开展业务或者其他渠道获取、加工和保存的个人信息，包括个人身份信息、财产信息、账户信息、信用信息、金融交易信息及其他反映特定个人某些情况的信息”，而这个定义，从文义解释来看，个人金融信息将与金融机构所处理的所有个人信息无限趋同。

然而，金融机构处理有关个人信息的行为，天然具有其特殊性。一方面，金融机构开展业务时会受到严格监管，在履行“了解你的客户”（KYC）义务以及面对反洗钱的要求时，其对信息的采集和处理就不能完全依赖于客户同意；另一方面，金融机构在采取技术手段进行反欺诈和反盗用时，如果仍严格要求其遵守用户同意的原则，则有可能给金融机构甚至国民经济带来重大负面影响。此外，即便是在以对个人信息严格保护著称的欧洲，其也并不将取得个人信息主体的同意视为解决问题的唯一路径，根据 GDPR 的有关规定，除取得信息主体的同意外，还存在为履行合同、履行法定义务所必须，保护信息主体或他人的重大利益所必须，为实现数据控制者所追求的合法利益所必须等其他合规路径。

为了解决法律规定与个人信息保护的现实困难之间的问题，GB/T 35273-2017《信息安全技术 个人信息安全规范》的 5.6 条对于征得授权同意的例外情况做出规定：“以下情形中，个人信息控制者收集、使用个人信息不必征得个人信息主体的授权同意：a) 与个人信息控制者履行法律法规规定的义务相关的；b) 与国家安全、国防安全直接相关的；c) 与公共安全、公共卫生、重大公共利益直接相关的；d) 与刑事侦查、起诉、审判和判决执行等直接相关的；e) 出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人授权同意的；f) 所涉及的个人信息是个人信息主体自行向社会公众公开的；g) 根据个人信息主体要求签订和履行合同所必需的；（注：个人信息保护政策的主要功能为公开个人信息控制者收集、使用个人信息范围和规则，不宜将其视为合同）h) 从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道；i) 维护所提供产品或服务的

安全稳定运行所必需的，如发现、处置产品或服务的故障；j)个人信息控制者为新闻单位，且其开展合法的新闻报道所必需的；k) 个人信息控制者为学术研究机构，出于公共利益开展统计或学术研究所必要，且其对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的。”

我们注意到，《技术规范》参照 GB/T 35273-2017《信息安全技术 个人信息安全规范》的有关规定，在 7.1.1d)款对征得授权同意的例外做出专门设定，其内容与 2017 年版《信息安全技术 个人信息安全规范》的规定基本相同，但是，在最后一项“用于维护所提供的金融产品或服务的安全稳定运行所必需的”情形中，特别举例包括“识别、处置金融产品或服务中的欺诈或被盗用等”情形。虽然有观点认为《技术规范》作为一个推荐性标准，此类例外原则的内容从某种程度上突破了上位法的规定，并因此对其效力存疑，但是，我们认为，这一规定真实反映了行业特点与行业的迫切需求，对国民经济和金融稳定而言具有正面意义，且并不一定会对个人信息保护工作带来很大的负面影响。考虑到我国的特殊国情，此类突破性的规定，是否能得到监管部门在今后立法及执法方面的认可和参考，尚具有很大的不确定性。

四、《技术规范》中关于个人金融信息的分类保护

如前所述，我国之前的立法对“个人金融信息”做了极为宽泛的定义，《技术规范》也不例外。根据《技术规范》的规定，“个人金融信息”是指“金融业机构通过提供金融产品和服务或者其他渠道获取、加工和保存的个人信息”，包括账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息及其他反映特定个人某些情况的信息。由于定义过于宽泛，而不同个人金融信息被泄露或滥用所带来的影响和危害不同，《技术规范》将个人金融信息按敏感程度从高到低分为 C3、C2、C1 三个类别，对不同类别的个人金融信息，做不同的规范性要求。

根据《技术规范》的规定，C3 类别信息主要为用户鉴别信息，包括银行卡磁道数据(或芯片等效信息)、卡片有效期等账户信息，及银行卡密码、交易密码，卡片验证码，用于用户鉴别的个人生物识别信息等鉴别信息；C2 类别信息主要为可识别特定个人金融信息主体身份与金融状况的个人金融信息，以及用于金融产品与服务的关键信息，包括但不限于支付账号及其等效信息、账户登录的用户名、用户鉴别辅助信息（若用户鉴别辅助信息与账号结合使用可直接完成用户鉴别，则属于 C3 类别信息）、个人财产信息、交易信息、个人金融信息主体照片、音视频等影像信息、家庭地址等能够识别出特定主体的信息；而 C2 和 C3 类别信息中未包含的其他个人金融信息将被划为 C1 类别信息。

对于 C3 类的信息，《技术规范》要求最为严格。根据《技术规范》的规定，不应委托或授权无金融业相关资质的机构收集 C3 类信息；传输应使用加密方式进行；不应留存非本机构的银行卡磁道数据(或芯片等效信息)、银行卡有效期、卡片验证码（CVN 和 CVN2）、银行卡密码、网络支付密码等 C3 类别信息，若确有必要留存的，应取得个人金融信息主体及账户管理机构的授权；不应委托给第三方机构进行处理；不应共享、转让、公开披露；约束外包服务机构与外部合作机构不应留存 C3 类别信息。

对于 C2 类的信息，除特别明确用户鉴别辅助信息不得委托第三方机构处理，不应共享、转让、公开披露之外，《技术规范》对于 C2 类信息，只是要求不应委托或授权无金融业相关资质的机构收集 C2 类信息，传输方式应当加密，且约束外包服务机构与外部合作机构不应留存 C2 类信息。

有观点认为，上述规定要求收集个人金融信息（C2/C3）的主体必须为金融业持牌机构（例如持牌的小贷公司、消金公司、征信机构等），而将其他非持牌机构（例如导流、助贷、大数据分析公司）排除在外。

我们对此持不同看法。首先，《技术规范》仅仅要求不应委托或授权上述机构收集 C3 类信息，但并未禁止用户委托或授权上述机构向金融机构提交此类信息；其次，禁止委托或授权上述机构收集，并不必然代表禁止有关第三方服务主体采集相关信息并输出相关验证结果；此外，正如本文第二部分的分析，对于需要取得资质的金融业机构而言，《技术规范》具有准规范性的效力，对于其他没有明确金融监管部门的行业而言，此类要求显然没有意义。

五、《技术规范》中关于个人生物识别信息的规定

2020 年 3 月 6 日，全国信息安全标准化技术委员会归口的 GB/T 35273-2020《信息安全技术个人信息安全规范》正式发布，并将于 2020 年 10 月 1 日实施。由于个人生物识别技术的普遍应用，且一旦发生信息安全事件，将对个人产生重大不利影响。新版《个人信息安全规范》对于个人生物识别信息做了特别的保护要求：第一，新版《个人信息安全规范》要求“收集个人生物识别信息前，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”；第二，“个人生物识别信息应与个人身份信息分开存储”；第三，“原则上不应存储原始个人生物识别信息（如样本、图像等），可采取的措施包括但不限于：1) 仅存储个人生物识别信息的摘要信息；2) 在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能；3) 在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像。”

《技术规范》中关于个人生物识别信息的要求与新版《个人信息安全规范》的规定也是互相呼应。首先，《技术规范》将“用于用户鉴别的个人生物识别信息”列为敏感度最高级别的 C3 类别信息，对其收集、传输、存储、使用和共享等各方面提出了最为严格的要求；其次，《技术规范》要求“受理终端、个人终端及客户端应用软件均不应存储银行卡磁道数据(或芯片等效信息)、银行卡有效期、卡片验证码(CVN 和 CVN2)、银行卡密码、网络支付密码等支付敏感信息及个人生物识别信息的样本数据、模板，仅可保存完成当前交易所必需的基本信息要素，并在完成交易后及时予以清除。”

六、结语

《技术规范》对个人金融信息的定义、分类，以及收集、传输、存储、使用、删除、销毁全生命周期进行了规定，还包括了安全制度体系建立与发布等内容，参考了大量的安全规范，其涉及的内容非常广泛。我们将持续关注《技术规范》在行业内的适用情况，并希望《技术规范》能够对将来的金融领域信息保护立法和执法带来积极的影响。（来源:《中国信息安全》杂志 2020 年第 4 期）

➢ 网络安全人才培养应遵循“防御升级，持续学习”理念

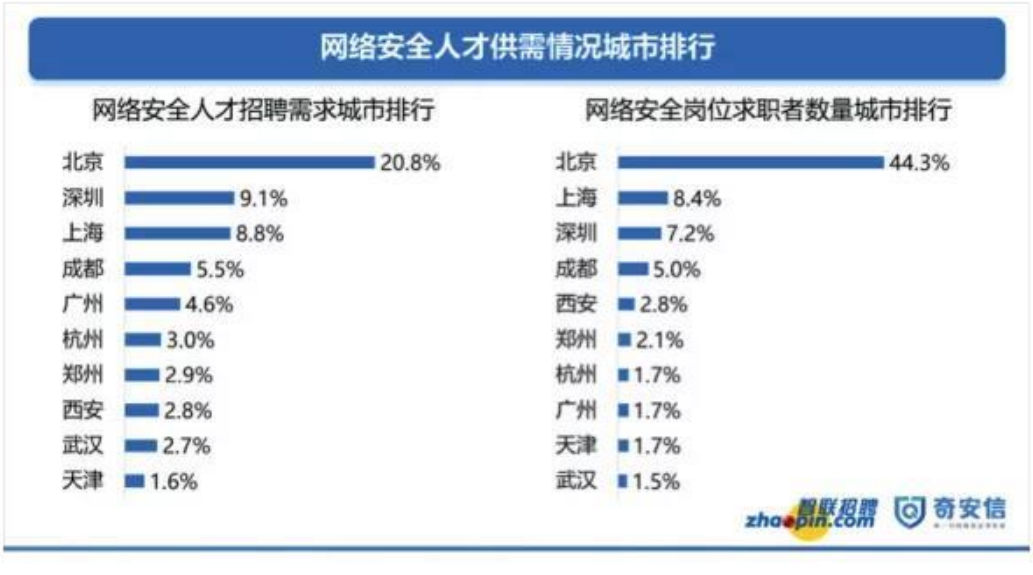
随着我国经济信息化程度的提升和数据资产的储备提升，网络安全不管对于国家、企业还是个人，都成了关乎核心权益的刚需。伴随着行业的快速发展，不管是产业发展的需要还是网络空间实力的打磨，网络安全建设的核心要素依然是网络安全人才。

一、网络安全人才需求呈现爆发式增长，人才需求分布城市下沉

根据智联招聘与奇安信在 2019 年发布的《2019 网络安全人才市场状况研究报告》显示，2019 年 6 月网络安全人才市场需求的规模达到 2016 年 1 月需求的 24.6 倍，相比 2018 年 7 月增长了 3 倍。

从安全人才需求的月度指数变化来看，2018 年下半年以来，11 月份出现第一个高峰，2019 年 6 月份则是第二个高峰。第一个高峰源自于 2018 年 10 月，公安部发布《公安机关互联网安全监督检查规定》，这一规定的出台客观上要求被检查单位必须建立常态化的安全队伍，切实建立安全保障体制机制；第二个高峰则是业界关注的“等保 2.0”发布的时间段，网信办和工信部颁布的相关安全管理规定，呼应了社会对网络与信息安全的关注，同时也对互联网企业、安全厂商、各大政企单位提出更高的安全合规要求，而这些制度的落实都离不开安全责任人的人才储备。

从人才需求特征来看，2019 年度网络安全人才市场呈现需求进一步增长、用人单位的地域分布进一步下沉、人才需求更加多样化、基础化、体系化（常态化）等特点。数据显示，北京、深圳、上海、成都、广州是网络安全人才需求量最大的城市，这五个城市对网络安全人才需求的总量占全国需求总量的 48.8%。相较于 2018 年需求量前五的城市占全国的 60.7%，2019 年的需求占比总和降低了约 16 个百分点，这表明更多地区加大了对网络安全的投入，增加了对网络安全人才的需求。



人随产业走，人才的流动也随着需求的扩散而进行重新分配，2019 年北京地区的求职者占比从去年的 59.4%下降至 44.3%，同时其他城市的求职者正在稳步上升。

二、人才缺口刺激企业高薪挖角，应用型、基础性网络安全人才需求更显迫切

从用人需求的行业分布来看，IT 信息技术和互联网行业是网络安全人才需求大户，分别占到了总量的 42.4%和 13.7%。需求排名第三的是制造业，招聘数量占比 12.3%。由于网络安全人才长期存在供给缺口，用人单位提供给安全人员的薪酬也普遍高于求职者的预期。统计显示，2017 年求职者期望的平均薪资约为 7533.5 元/月，2018 年为 8587.5 元/月，2019 年为 11263.9 元/月。而用人单位提供的网络安全相关岗位的平均招聘薪酬约为 11728.9 元/月，高于预期。

根据对用人单位的调研，了解到企业在招聘网络安全人才时，不再只关注网络安全高水平攻防的人才，而是更注重使用基础性网安人才，从全面构建安全防御能力的角度，逐步吸纳所需人才，组建网络安全专业队伍。通过对企业招聘岗位的统计分析发现，安全运营与服务类岗位需求量最多，占 32.7%，其次是研发与测试类岗位 25.0%，销售类占 11.7%。

基础性的安全人才对学历的要求不高，而是更注重实战能力。以安全运营人才为例，该角色并不需要高深的 IT 安全知识，也不需高超的挖洞能力，只需熟悉各类安全设备的基本特点，并熟悉操作配置等，就具备从事安全运营工作的基本条件，因此专科学历的毕业生就完全可以胜任。根据智联人才市场大数据的学历分布结构也能看到，2018-2019 年度的求职者学历分布上，大专学历人才的比例有所上升，即高职或大专层次的专业人才比重加大。

基础性安全人才与高学历、高智商挖洞人才的需求量，正在形成一个人才需求的“金字塔”结构。基础性的实践应用型人才即金字塔底座，而塔尖是高学历、能力超长的研究型、创新型人才。未来，随着各个行业对基础性网络安全人才的招募，那些既熟悉招聘企业业务，又熟悉安全业务，同时还能熟练使用市场上各种安全产品的复合型人才会更加抢手。

三、校企结合，实现学术与实践的高效整合

从网络安全人才的学科专业背景来看，仅有极少数求职者有网络安全或信息安全的学科教育背景，而更多的网络安全岗位求职者实际上是来自于计算机、电子信息工程、软件工程和网络工程等兄弟专业。这也再次说明，网络安全专业向市场输出的人才数量仍然有限。

同时，智联招聘大数据显示，培养网络安全人才的高校阵营也在进一步亲民化，重点高校不再是肩负人才培养责任的唯一群体，更多的省/市地方院校也加入培养网络安全人才的大军。通过对网络安全岗位求职者的毕业院校分析发现，毕业于河北科技学院、山西工商学院、郑州科技学院、中国石油大学的人才最多。其中，来自河北科技学院和山西工商学院这两所高校的网络安全岗位求职者，占了求职者总数的 1.49%。

近些年，国家非常重视网络安全人才的培养，《网络安全法》第二十条要求：“国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培

养网络安全人才，促进网络安全人才交流。”近年来，面对网络安全人才近百万的市场缺口，高等学校、安全企业、社会培训机构、相关科研机构和协会联盟等，都积极探索、实践多元化、协同联动的网络安全人才培养模式。目前我国高等院校的网络安全专业每年为社会培养输出的毕业生在 2 万人左右。而企业作为人才需求方，有实操条件，也有充分的动力一同参与到人才培养项目中来。校企的紧密合作可以在学术和实操两方面实现人才培养资源的互补。

四、网络安全人才培养要“严进严出”，职业操守尤为重要

网络安全人才被要求攻防兼备，非常考验人才的实操技术，这对教育机构来讲无疑是一大挑战，教育专家们在产学结合、技术竞赛、人才认证方面也在不断探索。

网络安全的实际工作突破主要依赖于员工技能的提升，技术竞赛是人才能力的有力补充，近些年，各大高校、团体等举办各种类型的安全类夺旗、攻防等竞技比赛，一方面可以以赛促学，培养选拔网络安全的专业能手；另一方面可以促进全社会更加关注重视网络安全。

但信息安全堡垒实际上更容易从内部突破，胜任网络安全岗位的人选应该具备基本的道德底线，满足“德才兼备”的标准。比如在网络安全人才道德培养及规范上，武大已经开设了心理测试用以评估学生人格健康，还在日常课程上设置刑法内容学习，结合犯罪案例对学生进行警示，并在考试中进行考核。

智联招聘作为人力资源服务企业，也拥有一套完善的人才测评体系，与中国科学院心理研究所组织与员工促进中心等权威机构全面合作，从“动机”、“胜任力”、“性格”、“能力”四个维度对候选人进行全面测评，帮助企业了解候选人的软实力。

智联招聘 CTO 李京峰曾针对网络安全产学结合方向提出过相关建议，他认为网络安全是矛和盾的问题，彼此是通过实操互相迭代升级的，因此网络安全人才培养应该秉持“防御升级，持续学习”的理念，以掌握最前沿的技术能力。预测未来 3-5 年内，具备实战技能的安全运维人员与高水平的网络安全专家，将成为网络安全人才市场中最为稀缺和抢手的资源。（来源:《中国信息安全》杂志 2020 年第 4 期）

四、政府之声

➢ 工信部发布《工业和信息化部关于工业大数据发展的指导意见》附解读

2020 年 5 月 13 日，工业和信息化部发布《关于工业大数据发展的指导意见》（工信部信发〔2020〕67 号，下称《指导意见》），现就《指导意见》有关内容解读如下：

一、什么是工业大数据？为什么要出台《指导意见》？

工业大数据是工业领域产品和服务全生命周期数据的总称，包括工业企业在研发设计、生产制造、经营管理、运维服务等环节中生成和使用的数据，以及工业互联网平台中的数据等。随着第四次工业革命的深入展开，工业大数据日渐成为工业发展最宝贵的战略资源，是推动制造业数字化、网络化、智能化发展的关键生产要素。全球主要国家和领军企业向工业大数据聚力发力，积极发展数据驱动的新型工业发展模式。

党中央、国务院高度重视大数据发展，强调推动大数据在工业中的应用。习近平总书记指出，要“构建以数据为关键要素的数字经济”“系统推进工业互联网基础设施和数据资源管理体系建设，发挥数据的基础资源作用和创新引擎作用。”《促进大数据发展行动纲要》《关于深化“互联网+先进制造业”发展工业互联网的指导意见》等政策文件均提出要促进工业大数据的发展和应用。今年 4 月，党中央、国务院印发《关于构建更加完善的要素市场化配置体制机制的意见》，明确提出要支持构建工业等领域规范化数据开发利用的场景，提升数据资源价值。

我国是全球第一制造大国，工业大数据资源极为丰富。近年来，随着新一代信息技术与

工业融合不断深化，特别是工业互联网创新发展，工业大数据应用迈出了从理念研究走向落地实施的关键步伐，在需求分析、流程优化、预测运维、能源管理等环节，数据驱动的工业新模式新业态不断涌现。但相比于互联网服务领域大数据应用的普及和成熟，工业大数据更加复杂，还面临数据采集汇聚不全面、流通共享不充分、开发应用不深化、治理安全短板突出等问题，总体上仍处于探索和起步阶段，亟待拓展和深化。

未来三到五年，随着 5G、工业互联网、人工智能等的发展，工业大数据将从探索起步阶段迈入纵深发展阶段，迎来快速发展的机遇期，全球工业大数据的竞争也将变得更为激烈。立足当前、着眼未来，制定出台《指导意见》意义重大。一是贯彻落实党中央、国务院工作部署的重要举措；二是有利于加快工业数字化转型进程；三是有利于凝聚各方共识，构建协同推进的工作体系，形成发展合力，着力解决突出问题，共建共创工业大数据生态。

二、《指导意见》是怎么编制的？总体考虑是什么？

《指导意见》编制过程如下：2019 年 4 月，我们组织中国信息通信研究院、国家工业信息安全发展研究中心、中国工业互联网研究院、中国电子信息产业发展研究院、中国电子技术标准化研究院、工业和信息化部电子第五研究所等单位组建文件编写组，启动《指导意见》编制工作。编写组在赴广东、浙江、江苏和北京等典型地区实地调研基础上，组织召开了工业企业、互联网企业、工业软件企业等参加的专题座谈会，就工业大数据和工业数字化转型等相关问题听取了近 50 家企业和院士、专家的意见，并就数据管理等专题听取了部分地方行业主管部门的建议，形成《指导意见》初稿。2019 年 8 月，我们征求了中央网络安全和信息化委员会办公室、国家发展改革委等相关部门意见，2019 年 9 月在工业和信息化部网站向社会公开征求意见，经认真研究，我们采纳了其中的合理建议，修改完善后形成了《指导意见》。

《指导意见》总体考虑如下：一是坚持全盘布局、系统推进。发展工业大数据是一项复杂的系统工程，既要构建工业大数据采集、汇聚、流通、分析、应用的价值闭环，推动创新发展，也要提升数据治理和安全防护能力，保障发展安全；既要重视在需求侧促进大数据与实际业务深度融合，也要在供给侧推动大数据技术和产业创新发展；既需要在宏观层面加强体系化布局，建立全面系统的工业大数据生态，也需要在微观层面务实着力，提升企业的数据管理能力。因此，《指导意见》的重点任务涉及数据汇聚、数据共享、数据应用、数据治理、数据安全、产业发展 6 个方面，能够全面支撑工业大数据发展。二是坚持问题导向、突出重点。工业大数据高度复杂，数据采集汇聚难、共享流通难、分析应用难、安全治理难，一蹴而就解决全部问题是不可行也不现实的。在广泛调研和深入研讨的基础上，《指导意见》

紧盯问题短板，抓住重点关键，针对我国工业大数据现阶段的发展特点、主要问题和亟待取得突破的重点领域，共设置了 18 项重点任务，精准施策，务实有序推动工业大数据发展。

三、当前工业数据采集汇聚存在哪些问题？《指导意见》提出了什么举措？

工业大数据的采集汇聚过程中面临的痛点较多。企业反应的主要问题包括：因企业信息化基础差、设备接口不开放等造成数据采集不上来；企业数据底账不清，不知道自己有哪些数据、分布在哪里，大部分工业数据处于“睡眠”状态；因设备不互联，通信协议不兼容等造成不同数据不匹配、不互认，数据孤岛现象普遍；数据失真、失准及一致性差等因素导致数据汇聚质量不高，等等。

《指导意见》部署了 3 项重点任务，推动全面采集、高效互通和高质量汇聚，包括加快工业企业信息化“补课”、推动工业设备数据接口开放、推动工业通信协议兼容化、组织开展工业数据资源调查“摸家底”、加快多源异构数据的融合和汇聚等具体手段，目的是为了形成完整贯通的高质量数据链，为更好地支撑企业在整体层面、在产业链维度推动全局性数字化转型奠定基础。

四、《指导意见》提出要统筹建设“国家工业大数据平台”的考虑是什么？

在国家层面把基础数据汇聚起来，建设以大数据为手段支撑政府精准施策、精准管理的平台，正变得日益重要。比如，在此次疫情爆发初期，针对重点物资保障需求不明、底数不清、对接不畅等困难，工业和信息化部依托制造强国产业基础大数据平台快速建成“国家重点医疗物资保障平台”，运用信息化手段保障重点医疗物资的科学调度、统筹平衡和高效供应，为打赢疫情防控阻击战提供有力支撑。《指导意见》部署了“建设国家工业互联网大数据中心”“建立多级联动的国家工业基础大数据库”等具体手段，以更好地服务政府决策和企业发展。

五、关于促进工业数据共享流通，《指导意见》有哪些举措？

随着新一代信息技术与工业融合从单点局部走向全局优化，工业企业对于跨企业、跨行业数据共享合作的需求正在快速增加。推动数据共享流通，促进数据要素市场化配置，也是 4 月党中央、国务院发布的文件《关于构建更加完善的要素市场化配置体制机制的意见》部署的重点任务。但目前，企业普遍反应，因数据权属界定不清、规则不明、难以定价等基础性问题没有得到解决，跨企业、跨行业的数据共享流通难以开展。这是一个全球性难题。《指导意见》部署了 2 项重点任务，通过探索建立工业数据空间、加快区块链等技术在数据流通中的应用、完善工业大数据资产价值评估体系等方式，从技术手段、定价机制、交易规则等多个方面着手，激发工业数据市场活力，促进数据市场化配置。

六、当前工业大数据应用中存在什么问题？《指导意见》如何促进工业大数据应用？

部分领军企业在数据应用上进行了深入探索，也取得了发展实效，但大量工业企业的数据应用仍然是单点的，局部的、低水平的。企业反映的原因包括：对数据的不重视，“不想用”；数据分析的手段、人才等缺乏，“不会用”；对数据应用规律缺乏认识，数据应用投入大，“不敢用”，等等。《指导意见》部署了 4 项重点任务，通过在需求端组织开展工业大数据应用试点示范、开展工业大数据竞赛等手段，解决不想用、不敢用等问题；通过在供给端培育海量工业 APP、工业大数据解决方案供应商、向中小企业开放数据服务能力、培育应用生态等手段，降低企业数据应用的成本投入和专业壁垒，解决不会用、不敢用问题。供需双向发力，共同推动工业大数据全面深度应用。

七、《指导意见》为什么强调要“开展数据管理能力评估贯标”？

目前工业大数据的顶层设计已经基本完备，落地实施的一个关键抓手在微观企业上：只有当千千万万的微观工业企业有能力管好、用好数据，工业大数据价值才能真正遍地开花。但当前，仍有大量工业企业对数据不重视，欠缺数据管理的意识和能力。从美国的经验和我国推进两化融合的经验来看，建立数据管理能力标准、然后引导企业进行贯标，是快速将数据驱动能力注入企业的行之有效的方法。《指导意见》强调推广《数据管理能力成熟度评估模型》（DCMM）国家标准，以贯标评估引导工业企业切实提升数据管理能力，为全面激发工业数据价值打下坚实微观基础。

八、在强化数据安全防护方面，《指导意见》有哪些重点举措？

工业数据已成为黑客攻击的重点目标。相关数据显示，我国 34%的联网工业设备存在高危漏洞，这些设备的厂商、型号、参数等信息长期遭恶意嗅探，仅在 2019 年上半年嗅探事件就高达 5151 万起。导致工业信息安全防护能力滞后于工业融合发展进程的原因，除了技术上传统 IT 信息安全系统无法有效防护工业数据安全外，工业数据安全责任体系建设方面的部分空白也是重要原因。此外，我国工业信息安全领域的企业规模普遍小，缺少龙头企业，产品竞争力不强。《指导意见》布局了 2 项重点任务，强调明确企业安全主体责任和各级政府监督管理责任，建立工业数据安全责任体系；支持安全产品开发，培育良好安全产业生态，多措并举创新和强化工业数据安全防护，筑好筑牢发展的底线和防线。

九、下一步，如何推动《指导意见》落实？

（一）组织宣贯培训。面向地方各级工业和信息化主管部门、事业单位、工业企业和工业互联网平台企业等，详细解读和宣贯《指导意见》内容。

（二）建立推进机制。会同工业和信息化部相关司局以及业内外资深专家等组建推进工

作机制，与各地工业和信息化主管部门做好对接，建立纵向联动、横向协同的推进工作机制，确保重点任务落实，及时沟通信息、交流经验。

（三）任务分解落实。抓紧制定形成可落地、可执行的重点任务分工表，落实推进责任。鼓励和指导地方工业和信息化主管部门结合区域特点，提出适合本地区实际情况的政策措施。

（四）开展试点示范。鼓励有条件的地方、行业和工业企业围绕数据共享流通、数据应用、数据管理能力评估、数据分级分类等重点任务先行先试，按照边试点、边总结、边推广的思路，探索可复制、可推广的实施路径和模式。（来源：中华人民共和国工业和信息化部）

- **《工业和信息化部关于工业大数据发展的指导意见》工信部信发〔2020〕67 号全文：**
- http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757022/c7909590/content.html

➢ 农业农村部印发《2020 年农业农村部网络安全和信息化工作要点》通知

2020 年 5 月 8 日，农业农村部印发《2020 年农业农村部网络安全和信息化工作要点》通知 农办市[2020]6 号。

通知提出，指导各级农业农村部门推动实施《数字农业农村发展规划(2019—2025 年)》。加快启动实施“互联网+”农产品出村进城工程。推进国家数字农业农村创新中心和重要农产品全产业链大数据建设，进一步优化数字农业试点县项目布局和设计；会同中央网信办开展数字乡村试点县建设。加快推动农村集体资产大数据资源共享，建设农村集体资产监管平台，提升农村集体资产监管水平。（来源：中华人民共和国农业农村部）

- **农业农村部办公厅关于印发《2020 年农业农村部网络安全和信息化工作要点》的通知**
- http://www.moa.gov.cn/govpublic/SCYJJXXS/202005/t20200509_6343435.htm

➢ 国家网信办启动 2020“清朗”专项行动

2020 年 5 月 22 日，为进一步规范网上信息传播秩序，切实维护广大人民群众切身利益，促使网络空间更加清朗，即日起，国家网信办在全国范围内启动为期 8 个月的 2020“清朗”专项行动。

近年来，全国网信系统持续加大网络生态治理力度，深入整治网上各类违法违规问题乱象，舆论生态总体向好，网络治理成效明显。但色情低俗、网络暴力、恶意营销、侵犯公民个人隐私等负面有害信息花样不断翻新，极易反弹反复，严重污染网络生态环境，影响青少年身心健康，网民反映强烈、举报不断。为回应广大群众关切，国家网信办决定今年继续开展“清朗”专项行动。

国家网信办有关负责人介绍，“清朗”专项行动全面覆盖各类网络传播渠道和平台，集中清理网上各类违法和不良信息。专项行动将出重拳、用真招，对有令不行、顶风作案的网站平台依法从严处理，并公开曝光典型案例，有效震慑违法违规行为。

国家网信办有关负责人表示，“清朗”专项行动是网络综合治理的一项基础性、长期性任务，下一步将继续加大整治力度，建立完善长效治理机制，坚决遏制网上违法和不良信息蔓延态势。同时欢迎广大网民、媒体和社会各界积极参与，向网站平台和有关部门举报相关问题，携手共建清朗网络空间。（来源：中国网信网）

➢ 央行部署 2020 年重点工作：加强金融业网络安全和信息化统筹指导

2020 年 5 月 18 日，人民银行 2020 年科技工作电视电话会议在北京召开。会议全面总结了 2019 年以来科技工作成果，深入分析了当前面临的形势与挑战，并就 2020 年重点工作作出部署。人民银行党委委员、副行长范一飞出席会议并讲话。

会议认为，2019 年以来，在人民银行党委领导下，科技条线干部职工积极担当作为，各项工作协调推进，成效显著。强化自身建设，提升人民银行科技履职能力。加强统筹指导，防范化解金融网络安全风险。加强规划监管，推动金融科技健康有序发展。深化标准应用，

标准化工作再上新台阶。有力应对新冠肺炎疫情冲击，确保金融基础设施平稳运行。

会议指出，新冠肺炎疫情既检验了“十三五”期间金融业科技发展成效，也暴露出一些短板和不足。金融数字化转型更为迫切，金融网络安全形势更为严峻，金融业科技治理任重道远。要客观分析新形势和新挑战，积极抓重点、补短板、强弱项。

会议要求，2020 年人民银行科技工作要以习近平新时代中国特色社会主义思想为指导，贯彻落实党中央、国务院决策部署和行党委工作要求，不断完善与现代央行制度相适应的科技体制机制。加强科技支撑，深入开展“数字央行”建设，提升金融服务水平和金融监管能力；加强金融业网络安全和信息化统筹指导，推动落实金融领域密码应用与创新发展，筑牢金融网络安全屏障；推动金融科技高质量发展，提升金融服务实体经济能力；推进 LEI 应用，优化标准供给，提升金融标准治理水平；突出党建引领，推进全面从严治党，加强党风廉政建设，打造忠诚、干净、担当的新时代高素质专业化科技干部队伍。

人民银行有关司局、单位负责同志，上海总部，各分行、营业管理部，各省会（首府）城市中心支行，副省级城市中心支行科技工作负责同志参加会议。（来源：中国人民银行）

五、本期重要漏洞实例

➢ Microsoft 发布 2020 年 5 月安全更新

发布日期：2020-05-12
更新日期：2020-04-12
描述：

CVE(CAN) ID: CNTA-2020-0008

微软发布了 2020 年 5 月份的月度例行安全公告，修复了其多款产品存在的 111 个安全漏洞。受影响的产品包括：Windows 10 1909 & WindowsServer v1909（78 个）、Windows 10 1903 & WindowsServer v1903（78 个）、Windows 10 1809 & WindowsServer 2019（75 个）、Windows 8.1 & Server 2012 R2（30 个）、Windows Server 2012（27 个）、Windows RT 8.1（29 个）、Microsoft Edge (EdgeHTML-based)（5 个）、Internet Explorer（7 个）和 Microsoft Office-related software（12 个）。利用上述漏洞，攻击者可以获取敏感信息，提升权限，欺骗，绕过安全功能限制，执行远程代码，或进行拒绝服务攻击等。

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-2020-1126	**Media Foundation 内存破坏漏洞** 当 Windows Media Foundation 未能正确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。 攻击者有多种方法可以利用此漏洞进行攻击，例如说服用户打开精心编制的文档，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, version 1803 Server, version 1903 Server, version 1909 Server 2016 Server 2019
CVE-2020-1118	**Microsoft Windows Transport Layer 拒绝服务漏洞** 当传输层安全（TLS）的 Windows 实现未能正确地处理某些密钥交换时，存在拒绝服务漏洞。成功利用此漏洞的攻击者可导致目标系统停止响应。 要利用此漏洞，未经验证的远程攻击者可以使用 TLS 1.2 或更低版本向目标系统发送精心编制的请求，从而触发系统自动重新启动。 更新通过更改验证 TLS 密钥交换消息的方式来解决该漏洞。	重要 拒绝服务	Windows 10 Server, version 1803 Server, version 1903 Server, version 1909 Server 2019

CVE-2020-1153	**Microsoft Graphics 组件远程代码执行漏洞** Microsoft Graphics 组件处理内存中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在目标系统上执行任意代码。 要利用此漏洞，用户必须打开精心编制的文件。 安全更新通过更正 Microsoft 图形组件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, version 1803 Server, version 1903 Server, version 1909 Server 2016 Server 2019 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-1112	**Windows Background Intelligent Transfer Service 权限提升漏洞** 当 Windows Background Intelligent Transfer Service (BITS) IIS 模块未能正确地处理上传的内容时，存在权限提升漏洞。成功利用此漏洞的攻击者可以将受限制的文件类型上载到以 IIS 为主机的文件夹。 要利用此漏洞，攻击者将需要通过 BITS 上载文件的权限。然后，攻击者可以提交构建的文件上传请求。 安全更新通过更正 Windows BITS 如何验证文件名来解决该漏洞。	重要 特权提升	Windows 10 Server, version 1803 Server, version 1903 Server, version 1909 Server 2016 Server 2019 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-1174	**Jet Database Engine 远程代码执行漏洞** 当 Windows Jet 数据库引擎未能正确地处理内存中的对象时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在受攻击系统上执行任意代码。 攻击者可以通过诱使受害者打开精心编制的文件来利用此漏洞进行攻击。 更新通过更正 Windows Jet 数据库引擎处理内存中对象的方式来解决该漏洞。	重要 远程执行代码	Windows 10 Server, version 1803 Server, version 1903 Server, version 1909 Server 2016 Server 2019 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-1037	**Chakra Scripting Engine 内存破坏漏洞** Chakra 脚本引擎处理 Microsoft Edge (HTML-based)内存中对象的方式存在远程代码执行漏洞。该漏洞可能会破坏内存，使得攻击者可以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，则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。 在基于 web 的攻击场景中，攻击者可以托管精心编制的网站，该网站旨在通过 Microsof	严重 远程执行代码	Edge (EdgeHTML-based) ChakraCore

	t Edge (HTML-based)利用该漏洞，然后说服用户查看该网站。攻击者还可以利用受攻击的网站以及接受或承载用户提供的内容或广告的网站。这些网站可能包含精心编制的可利用此漏洞的内容。 安全更新通过修改 Chakra 脚本引擎如何处理内存中的对象来解决该漏洞。		
CVE-2020-1062	**Internet Explorer 内存破坏漏洞** 当 Internet Explorer 未能正确访问内存中的对象时，存在远程代码执行漏洞。该漏洞可能会破坏内存，使得攻击者可以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，则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 Internet Explorer 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 9 Internet Explorer 11
CVE-2020-0901	**Microsoft Excel 远程代码执行漏洞** 当软件未能正确处理内存中的对象时，Microsoft Excel 软件中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，则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。将帐户配置为在系统上拥有较少用户权限的用户可能比使用管理用户权限操作的用户受影响更小。 安全更新通过更正 Microsoft Excel 如何处理内存中的对象来解决此漏洞。	重要 远程执行代码	Excel 2010 Excel 2013 Excel 2016 Office 2019 Office 2016 for Mac Office 2019 for Mac 365 Apps Enterprise* formerly Office 365 ProPlus
CVE-2020-1069	**Microsoft SharePoint Server 远程代码执行漏洞** 当 Microsoft SharePoint Server 未能正确识别和筛选不安全的 ASP.Net web 控件时，存在远程代码执行漏洞。成功利用此漏洞的经过身份验证的攻击者可以使用精心编制的页面在 SharePoint 应用程序池进程的安全上下文中执行操作。 要利用此漏洞，经过身份验证的用户必须在受影响的 Microsoft SharePoint Server 版本上创建并调用构建的页面。	严重 远程执行代码	SharePoint Foundation 2013 SharePoint Enterprise Server 2016 SharePoint Server 2019

	安全更新通过更正 Microsoft SharePoint Server 处理已创建内容的方式来解决此漏洞。		

建议：

厂商补丁：
https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-May

➢ Mysql jdbc 驱动存在 XML 实体注入漏洞

发布日期：2020-05-13
更新日期：2020-05-13
受影响系统：
MySQL AB Mysql jdbc
描述：

CVE(CAN) ID: CNVD-2020-27158
MySQL AB 是由 MySQL 创始人和主要开发人创办的公司。
Mysql jdbc 驱动存在 XML 实体注入漏洞，攻击者可利用该漏洞获取服务器权限。*>
建议：

厂商补丁：
MySQL
目前，厂商尚未提供修复方案，请关注厂商主页更新：
https://www.mysql.com/

➢ 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。

<*来源：kay

*>

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/

➢ Adobe Character Animator 任意代码执行漏洞

发布日期：2020-05-19

更新日期：2020-05-20

受影响系统：

Adobe Character Animator <= 2020 3.2

描述：

CVE(CAN) ID: CVE-2020-9586

Adobe Character Animator 是一款直观的 2D 角色动画应用程序。

Adobe Character Animator 2020 3.2 及更早版本，在实现上存在缓冲区溢出漏洞，攻击者利用此漏洞可远程执行任意代码。

<*来源：Mat Powell

链接：https://helpx.adobe.com/security/products/character_animator/apsb20-25.html

*>

建议：

厂商补丁：

Adobe

Adobe 已经为此发布了一个安全公告（APSB20-25）以及相应补丁：

APSB20-25：Security Updates Available for Adobe Character Animator

链接：https://helpx.adobe.com/security/products/character_animator/apsb20-25.html

六、本期网络安全事件

➢ 欧洲多台超级计算机中毒 沦为挖矿肉鸡

2020 年 5 月 17 日，本周，欧洲突然曝出多达十数台超级计算机感染恶意挖矿软件，沦为挖矿肉鸡。据悉周一英国爱丁堡大学首先公布了 ARCHER 超级计算机遭到攻击的报告，表示关闭 ARCHER 的系统进行调查，并且为了防止再次被攻击，重置了 SSH（安全外壳协议）密码。

同一天德国超级计算机管理组织 bwHPC 宣布因为类似的安全问题，旗下 5 台超级计算机/高性能计算集群 bwUniCluster 2.0、ForHLR II、bwForCluster JUSTUS、bwForCluster BinAC、Hawk 现起关闭。

本周三安全研究员 Felix von Leitner 在博客中称，位于西班牙巴塞罗那的一台超级计算机也受到安全问题的影响，因此被关闭。

周四更多被感染的超级计算机浮出水面，巴伐利亚科学院下属的莱布尼兹计算中心当天表示因为安全漏洞，其管理的计算集群断开互联网连接。

当天晚些时候，德国朱利希研究中心紧接着表示由于发生“IT 安全事件”，必须关闭旗下 JURECA，JUDAC 和 JUWELS 超级计算机。

就在昨天瑞士苏黎世的瑞士科学计算中心也表示在直到外部环境安全之前，将持续关闭

其超级计算机的外部访问。

目前尚不清楚究竟是什么人或组织实施了这些攻击，但据安全公司分析，黑客是通过窃取 SSH 凭证获得了超级计算机的访问权限，而大学内部人士因为有权访问这些超级计算机而最有嫌疑。

实际上被劫持的 SSH 登录名分别属于加拿大、中国和波兰的大学。而且虽然没有证据证明所有的攻击都是由同一组织实施的，但所有恶意软件的文件名和网络指示器都证明它们的源头可能是同一个地方。（来源：快科技）

➢ 武汉多个小区居民核酸检测被拍手持身份证照 涉违规收集个人信息

2020 年 5 月 18 日，陆续有网友反映，所在小区组织做核酸检测时被工作人员要求手持身份证拍照，担心个人信息泄露。17 日晚，江岸区新冠肺炎疫情防控指挥部回应称，系涉事小区自行决定，目前已制止，照片也已完全删除。记者搜索发现，除了通报里提到的一个小区，武汉还有多个小区存在类似情况。对此，有律师表示，社区收集上述信息没有必要，而且如果社区是否具备收集和处理个人信息的能力存疑，极易导致个人信息的泄露风险。

武汉多个小区居民被要求手持身份证拍照

尽管当前武汉全市疫情防控形势趋于平稳，但每日仍有新发现的无症状感染者。为了全力阻断可能的传染源，消除社会恐惧和偏见，5 月 14 日，武汉市部署在全市范围内开展集中核酸检测。

按照要求，居民将按照属地化原则，到居住地所在社区的采样点进行采样。采样时，需带上本人身份证或户口本等有效证件，按照社区统一安排，预约前往。据悉，所有核酸筛查结果将汇总到独立的专用系统保存，确保受检居民个人信息安全。

然而，多个来自不同小区的网友都在做核酸检测时被工作人员要求手持身份证拍照。据记者不完全统计，江岸区的融科天城二期小区、解放大道光荣坊社区、西马街江北社区和江汉路某小区都有类似情况。

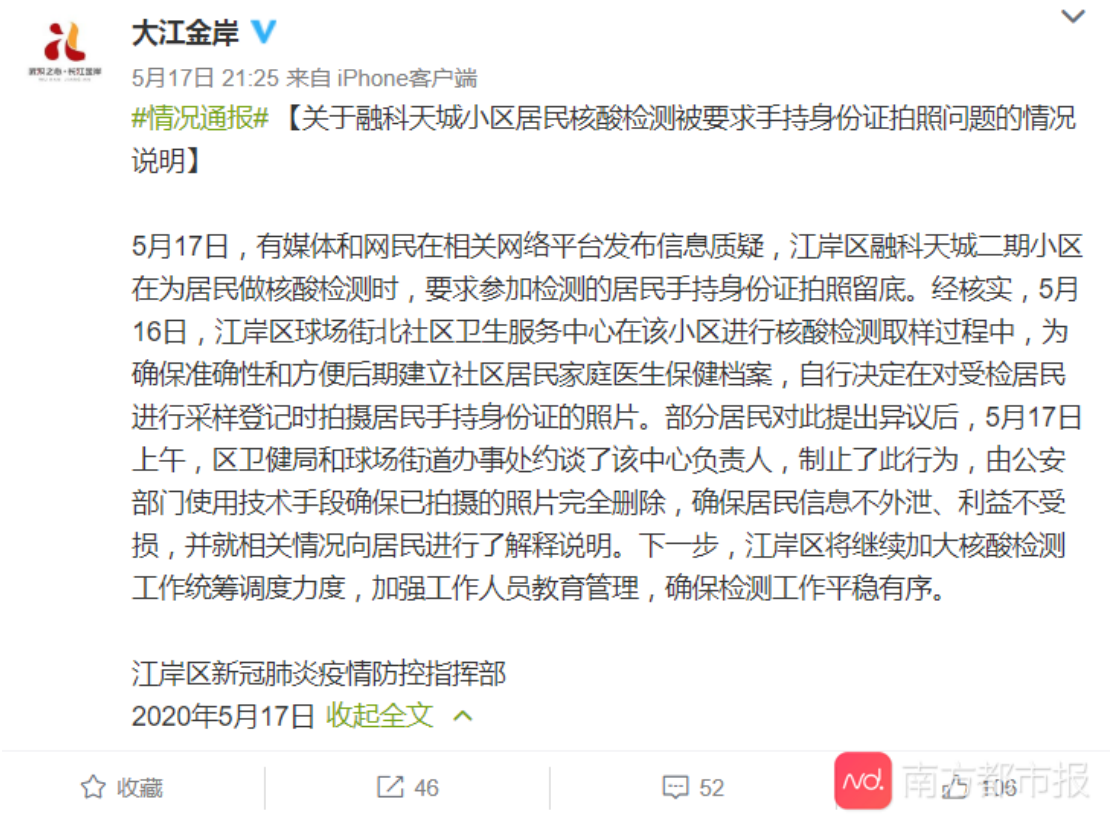
网友@千夕丨莺时记发博称，她所在小区除了要求手持身份证，还要持写有个人详细信息的纸条拍照。“甚至有工作人员在现场多次强调 在个人信息的纸条上要写清楚详细楼栋单元房号。”

她提到，检测流程是现在网格群填写个人资料，再去小区检测点排队。进场前需要填写

一张登记个人详细信息的纸条，排到自己后要先“登记”，即“坐在凳子上手持身份证+个人信息纸条拍照”，然后再做核酸检测。“大家都以为是国家要求的核酸检测前统计流程，哪怕觉得不对劲，也都配合了……谁知道是有些人夹带私货，未经允许来收集的个人信息……”，她写道。

曝光后，居民才意识到拍照行为不合理

5 月 17 日，武汉市江岸区官方微博@大江金岸就江岸区融科天城二期小区要求参加核酸检测的居民手持身份证拍照留底发布通报，称江岸区球场街北社区卫生服务中心为确保准确性和方便后期建立社区居民家庭医生保健档案，自行决定在对受检居民进行采样登记时拍摄居民手持身份证的照片。



通报还提到，部分居民对此提出异议后，区卫健局和球场街道办事处约谈了该中心负责人并制止了此行为。目前由公安部门使用技术手段确保已拍摄的照片完全删除，确保居民信息不外泄、利益不受损。新闻曝光之后，不少此前没有意识到个人权益被侵犯的网友也纷纷发言质疑，要求所属检测点给出合理解释和处理方案。

@是丹爷嘎说，“今天在小区排队做核酸检测，本来觉得挺好，到后来在群里看到大家都在讨论为什么要手持身份证拍照，才意识到这个信息泄漏的问题，对呀，为什么要手持身份证拍照？谁能出来给个解释，而且很多检测点是没有这个要求。希望能有合理的解释和处

理方案。”

专家：社区收集人脸信息没有必要

国家标准《信息安全技术 个人信息安全规范》要求，收集个人信息应遵循“最少必要”原则，个人信息控制者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。显然，做核酸检测收集手持身份证照片不符合上述要求。

北京玺泽律师事务所高级合伙人程贞也对记者表示，这些小区的做法很有问题，主要涉及三个方面。

一是收集个人敏感信息的必要性。做核酸检验时，现场就能进行验明身份的工作，不必收集身份证或面部识别信息等敏感个人信息。二是信息收集是否符合透明性和明确同意原则，即收集个人敏感信息时必须明确告知个人信息主体收集目的、使用、存储方式和安全处理措施等等，并得到个人信息主体明确的同意。

“如果没有告知的情况下，收集个人信息是违法的”，她强调，最后就是安全保障等技术和管理措施的问题。“社区是否具备这种能力来收集和处理个人信息是一个大大的问号，如果这方面能力欠缺，则会存在泄露个人信息的极大风险。”（来源：南方都市报）

➢ 英国易捷航空遭黑客入侵 约 900 万客户个人信息被窃取

2020 年 5 月 20 日，英国廉价航空公司易捷航空 EasyJet 的一份声明称，在一次重大数据泄露事件中，约 900 万客户个人信息被窃取，其中包括 2200 名客户的信用卡详细信息也被获取，但护照记录暂未发现泄露。易捷航空没有透露安全事件是何时发生的，也没有说明黑客是如何进入其系统的。

公司表示，已经将泄密事件提交给了英国的数据保护机构信息专员办公室(Information Commission's Office)。根据欧洲数据保护规则，公司有 72 小时的时间向监管机构通报安全事件。

和航空业的其他公司一样，这家航空公司也受到了冠状病毒大流行的沉重打击，疫情迫使全球大量人口呆在家里，商务旅行和度假被大量搁置。

在 COVID-19 大流行之前，EasyJet 在 2019 年运送了超过 2800 万名乘客，EasyJet 也是首批向英国政府请求救助以防止财务崩溃的公司之一。

英国监管机构 ICO 去年表示，在一次数据泄露暴露了 50 万客户的预订细节后，打算对英国航空公司(British Airways)处以创纪录的 1.83 亿英镑(约合 2.3 亿美元)的罚款，原因是黑客在其网站上安装了 Skiming 恶意软件后，盗走了数千个客户信用卡号码。（来源：cnBeta）

➢ 建行员工贩卖客户信息 5 万多条称不知违法

2020 年 5 月 21 日，日前，建设银行员工因参与黑色产业链、售卖客户个人信息被逮捕。记者从江苏淮阴市淮安警方获悉，近期破获了一起特大贩卖公民个人信息案。共抓获 26 名嫌疑人，涉案金额 2000 多万元，涉及公民个人信息 50000 多条。

其中，建设银行员工在黑色链条中发挥重要作用，将相关银行卡使用人的身份信息、电

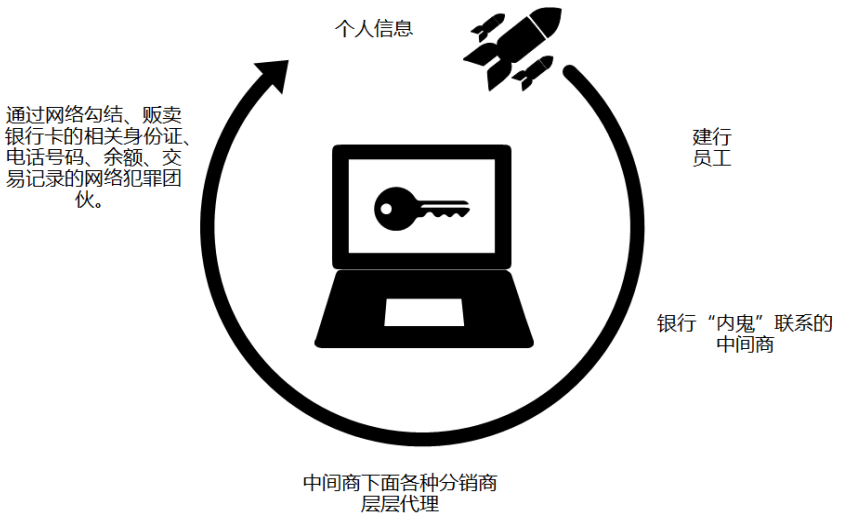
话号码、余额甚至交易记录，售卖给下家，进行谋利。“银行员工将个人账户信息泄露出去谋利，因涉及客户的资金安全，已不属于侵犯普通隐私的范畴，情节更加严重、恶劣。”一位业内人士对记者表示。

一条个人信息卖 80～110 元

近日，江苏淮阴市淮安警方在“净网 2019”专项行动中成功破获一起特大侵犯公民个人信息案件。该案涉及 9 个省份，公安部将此案列为部督专案。淮阴分局共抓获犯罪嫌疑人 26 名，扣押涉案手机 60 余部，涉案金额 2100 余万元，追缴违法所得 400 余万元，摧毁了 6 条泄漏、贩卖公民个人信息的黑色产业链。

早在 2019 年 6 月，有人在网上通过 QQ 等通讯工具公开出售银行卡相关信息，包括银行卡对应的卡主身份证号码、电话号码、余额甚至交易流水，引起了警方注意。警方注意到，QQ 群内昵称为“建行”、“在野”、“金融”等多个 QQ 号，长期在各个 QQ 群内发送广告，声称只要提供银行卡号或者身份证号，就可以查询到相关银行卡使用人的身份信息、电话号码、余额甚至交易记录。民警还发现，群内成员与这些 QQ 号私下交易，获得的信息又快又准。

一位男子王某称，在一个偶然的机会，他发现与银行卡相关信息售价动辄几百元，且需求量很大，于是他转行当起了“信息贩子”。接下来，他根据客户需要查询的不同银行卡，对应不同的上线查询渠道，并以经济利益诱惑，将建设银行一名员工拉下水。**建设银行这名员工供述**，根据双方达成“合作”协议，他每查询 1 条银行卡相关信息，即可获利 80～100 元不等的报酬。光凭这一黑色收入，建设银行员工年收入就超过 30 多万元。上述建设银行员工还称：“只知道售卖个人信息的做法违背银行的规定，不知道这种做法会违法。”



淮阴分局网安大队大队长朱延亮称

因为层级很多，所以越到产业链的末端，信息的价格越高，从“内鬼”到销售末端，一条信息的价格可能翻上数倍，除了犯罪风险，没有其他成本，利润非常高。淮阴警方称，目前，26 名犯罪嫌疑人已被移交检察机关提起公诉。

拿什么保护公民个人隐私

商业银行等金融机构掌握着大量用户，并且拥有非常关键的资金信息数据，但如果因为保护不善，导致个人信息泄露，将带来财产损失等个人影响，近期多起案件引发公众担忧。一位银行业人士称，个人信息售卖可以短期、快速获利，当前，银行在个人信息安全保护制度上还有待健全，疏于对员工的管理，再加上员工法律意识淡薄，使得泄漏现象屡禁不止。

北京盈科律师事务所合伙人唐春林对记者称：金融领域与其他领域相比，其业务规则和法律的联系更为紧密。通常，都是在法律有了原则性规定的情形下，金融监管部门和金融机构对具体执行做出细化，违反这些规定，大多数时候就意味着实质上违反了法律的规定，将产生相应的刑事责任、行政责任，甚至赔偿责任。但银行从业人员，很多时候对于这些规定缺乏清楚的认识，而违反法律规定的处罚，并不会因为无知而豁免，这样的教训是深刻的，应当引以为鉴。

唐春林称，银行等金融机构的工作人员，应当加强与自己业务相关的法律知识培训和学习。同时，银行应该将法律知识的学习和业务能力的培训，放在同等重要的位置。一旦触及法律的底线，不但影响业务的开展，更会使民众失去对金融机构的信任，其现实和长远的不利影响都是显而易见的。

“在法律的原则性规定下，监管部门各种细化性的规定会相应出台，不同部门、不同时期都会有指导意见、通知、规定等规范性文件。相关部门，应当做好规范性文件的清理、整理工作，以规范的行为或事件为对象，形成较为统一、系统的规定，以使相关人员查找方便，更易学习和理解。”唐春林建议称。

苏宁金融研究院高级研究员黄大智对记者表示：近年来，央行和银保监会不断加强对消费者的保护，但需要一个持久的过程。2019 年 12 月，央行起草了《中国人民银行金融消费者权益保护实施办法（征求意见稿）》，向社会公开征求意见，正式实施后，规范将升级到部门规章级别上。相信经过最近这一系列事情之后，国家会加速出台对公民信息保护的法律，强制性、有约束性的规范和措施将会出现。（来源：新华社）

➢ 江苏商家违法收集 2 万多人脸信息被罚

2020 年 5 月 15 日，日前，江苏省宿迁市一家健身中心因违法收集会员人脸照片信息，被宿迁市公安局宿豫分局责令限期整改，并处警告。这也是全国范围内，因违法收集人脸信息被处罚的案件首次公开曝光。有业内专家表示，该案具有“标杆意义”。

疫情催生健身热 民警日常检查发现违法线索

宿迁市公安局网安支队二大队副大队长郑舒舒告诉记者，在“净网 2020”的大背景下，公安机关网安部门一方面重点打击非法获取、出售公民个人信息的违法犯罪行为，另一方面也对重点行业、单位加强监督检查力度，对不履行个人信息保护义务的单位及时进行查处。他介绍，受新冠肺炎疫情影响，广大群众的健身意识有所增强，去健身场所锻炼的人越来越多。宿豫分局网安大队民警在日常工作中发现，一些健身场所因为会员管理和运营需要，收集了包括姓名、手机号码、年龄等在内的大量个人信息，甚至是人脸照片、指纹等个人敏感信息。

“有些健身场所收集存储了会员的人脸照片，在出入口使用了基于人脸识别技术的闸机通道。‘人脸闸机’的使用确实给会员带来便利，也降低了健身场所的运营管理成本，但同时也带来一些安全隐患。”郑舒舒说。

健身中心违法收集 2 万多名会员的人脸信息

今年 4 月，宿迁市公安局宿豫分局网安大队按照《公安机关互联网安全监督检查规定》

的要求，对一家健身中心进行了现场监督检查。调查发现，这家健身中心有 5 家门店，共收集存储了 20000 多名会员的姓名、手机号码、人脸照片、指纹等个人信息。

郑舒舒介绍，这家健身中心涉及的网络安全违法行为主要有两个，其一是未履行网络安全保护义务。“具体来说，这个健身中心没有网络安全方面的管理制度和负责人，对使用的信息系统没有开展网络安全等级保护定级备案和安全测评，特别是没有个人信息保护方面的制度和规定。”

其二是未履行个人信息保护义务，在收集会员姓名、手机号码，特别是人脸照片、指纹等个人敏感信息的时候，没有向会员明确说明收集、使用这些信息的目的、用途，并取得会员的同意，同时对收集和存储的这些信息也没有采取防范网络攻击、网络入侵以及数据加密等安全保护技术措施，很容易造成信息泄露的后果。

5 月 7 日，宿迁市公安局宿豫分局根据《中华人民共和国网络安全法》第四十一条、第四十二条第二款、第六十四条第一款之规定，对这家健身中心责令限期三十日内进行整改，并予以警告处罚。按照相关规定，整改期限届满后，公安机关还将对该健身中心的整改情况进行复查。

警方提醒：造成用户个人信息泄露或入刑

郑舒舒告诉记者，该案是宿迁市首次有单位因违法“采集人脸”被公安机关处罚。根据梳理公开资料发现，在江苏全省乃至全国，均没有线下商家因违法违规收集人脸信息被公安机关处罚的公开先例。此前，曾有一些线上 App 被有关部门约谈或处罚。例如在 2019 年 9 月，有网友发现一款名为“ZAO”的换脸应用要求获得用户的“人脸使用永久权”、隐私协议不规范，引发舆论热议。ZAO 开发公司的负责人随后被工信部问询约谈。

郑舒舒表示，从以往的案件侦办情况来看，线下商家违法违规收集公民个人信息，造成个人信息泄露或非法提供、出售公民个人信息的情况，其实也比较突出。

“公安机关积极主动作为，值得称道。”《信息安全技术个人信息安全规范》起草人之一、中国信息安全研究院副院长左晓栋认为，宿迁的这一案件“具有标杆意义”。

北京安理律师事务所高级合伙人王新锐告诉南都记者，加强个人生物识别信息的保护是国际趋势，中国的监管和执法机构对此也非常重视。目前，企业对于生物识别信息的重视程度还不够，在收集环节非常随意，而且往往直接收集并存储原始信息，存在较大的信息泄露的风险。

“这个案子带来的警示是，在个人信息收集、存储、使用等方面如处理不当，企业除了需民事责任以外，还可能面临行政处罚，甚至承担刑事责任的风险。涉及到人脸、指纹这些

生物识别信息的收集和使用，一定要慎之又慎。”王新锐说。

郑舒舒则提醒：依照《中华人民共和国网络安全法》和新修订的《信息安全技术 个人信息安全规范》（2020 年 10 月 1 日起施行）的规定，网络运营者在收集个人信息前，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。否则，将由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款等措施。情节严重的，还可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。此外，经监管部门责令采取改正措施而拒不改正，致使用户信息泄露，造成严重后果的，可能因涉嫌拒不履行信息网络安全管理义务罪，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金。

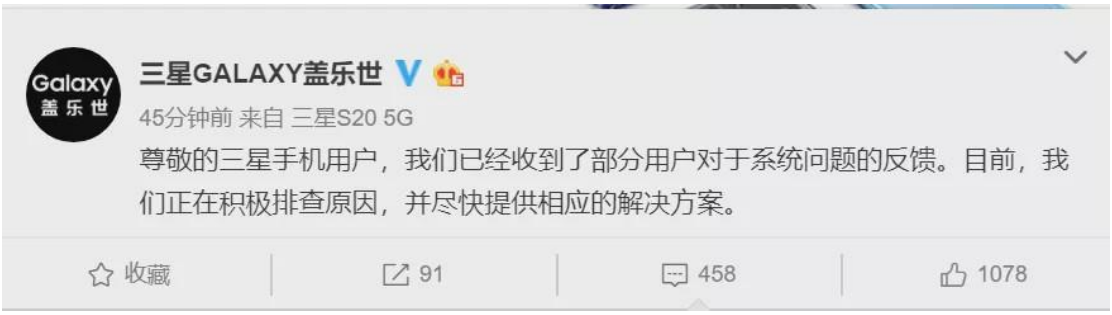
作为普通的公民、用户，该怎样保护自己的个人信息？“遇到有被收集个人信息特别是人脸、指纹、声纹等敏感信息的时候，一定要问清对方收集这些个人信息的目的、使用方式、范围、以及存储这些信息的安全措施。如果对被收集的个人信息后认为有误或者有异议，可以要求对方更正或者删除。“郑舒舒说。（来源：腾讯科技）

➢ 黑屏、乱码 三星手机大面积崩溃!官方紧急回应

2020 年 5 月 23 日，凌晨，忽然有大量使用三星手机的用户，在社交平台上发文称自己的三星手机，遭遇了三星手机系统崩溃，出现黑屏、乱码、无限重启等情况。已经没有办法维持设备的正常使用。而受影响机型包括三星 s8，s9，s10，乃至 s20 也受到了这次的影响。其中三星 s8，s9，s10 受影响极为严重。

其实，三星系统不止一次出现过此类问题。早在去年 Note10+开售后没多久，就有不少网友反映该机存在触控失灵的 BUG。但由于影响范围不算太大，三星并没有引起重视，时至今日三星才算是解决了这一 BUG。

中午，三星官方对此回应称，目前，我们正在积极排查原因，并尽快提供相应的解决方案。



今有分析认为，出现这样的情况，可能是三星的服务器遭遇了攻击。

有网友推断，三星手机应该是遇到时间 bug 或服务器崩溃，解决方法是关闭自动更新（关闭“通过 WLAN 自动下载”）、备份手机资料、重启时进桌面将时间改为 5 月 1 日。

据报道，有手机维修人员表示，目前圈内已经定位出问题，导致问题产生的软件为锁屏 APP，导致锁屏 APP 出现 bug 的是农历闰 4 月，出现该 bug 的为旧版锁屏 APP。“符合以上三种情况，锁屏以后即无限黑屏+重启。”同时，该业内人士的建议是，三星手机用户最好更新一下锁屏程序。（来源：中国经济网）