国盟信息安全通报

2020 年 6 月 21 日第 218 期

全国售后服务中心

国盟信息安全通报

（第 218 期）

国际信息安全学习联盟

2020 年 06 月 21 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 563 个，其中高危漏洞 211 个、中危漏洞 294 个、低危漏洞 58 个。漏洞平均分值为 6.08。本周收录的漏洞中，涉及 0day 漏洞 239 个（占 42%），其中互联网上出现“Subrion CMS 跨站请求伪造漏洞（CNVD-2020-32357）、Subrion CMS 跨站脚本漏洞（CNVD-2020-32356）”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 2100 个，与上周（3065 个）环比减少 31%。

主要内容

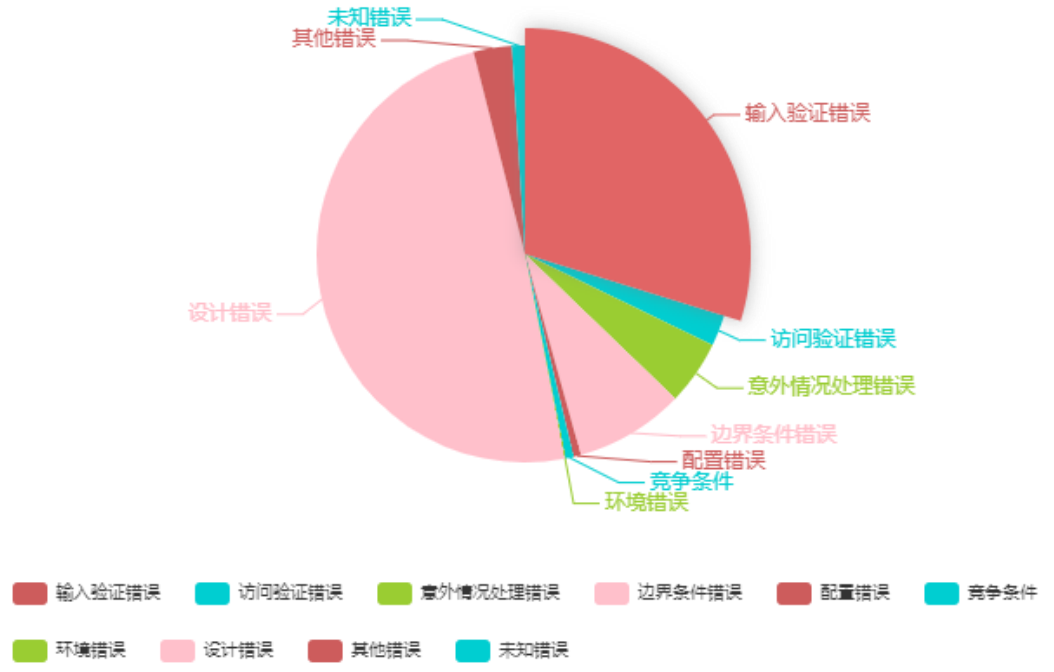
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

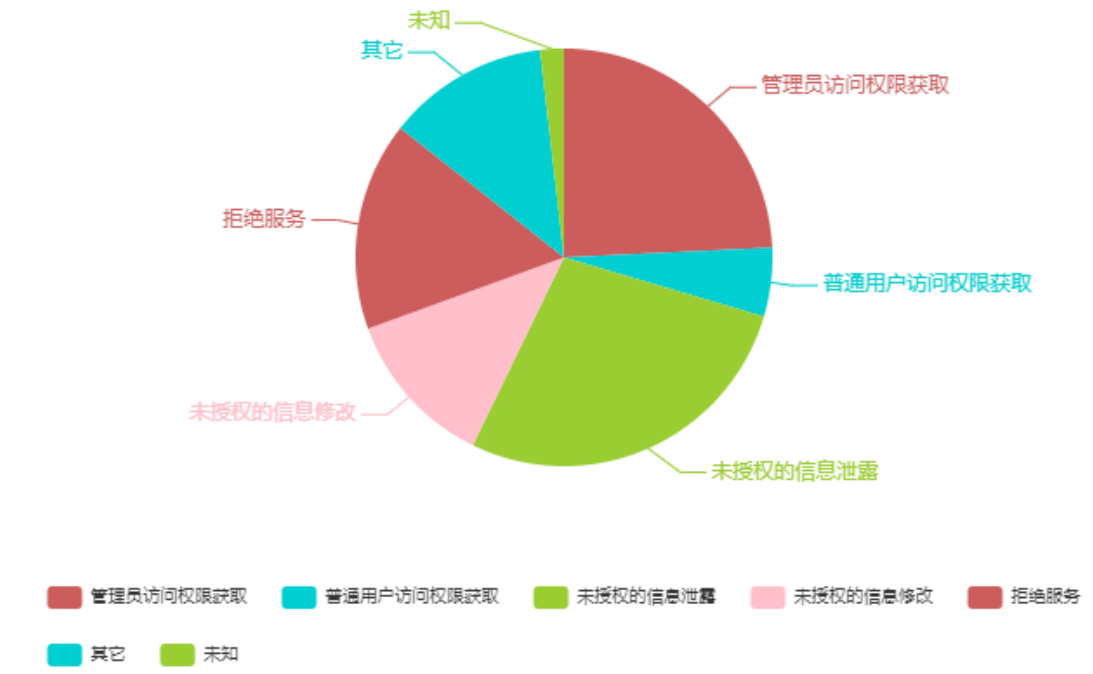
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 563 个，其中高危漏洞 211 个、中危漏洞 294 个、低危漏洞 58 个。漏洞平均分值为 6.08。本周收录的漏洞中，涉及 0day 漏洞 239 个（占 42%），其中互联网上出现“Subrion CMS 跨站请求伪造漏洞（CNVD-2020-32357）、Subrion CMS 跨站脚本漏洞（CNVD-2020-32356）”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 2100 个，与上周（3065 个）环比减少 31%。

二、安全漏洞增长数量及种类分布情况

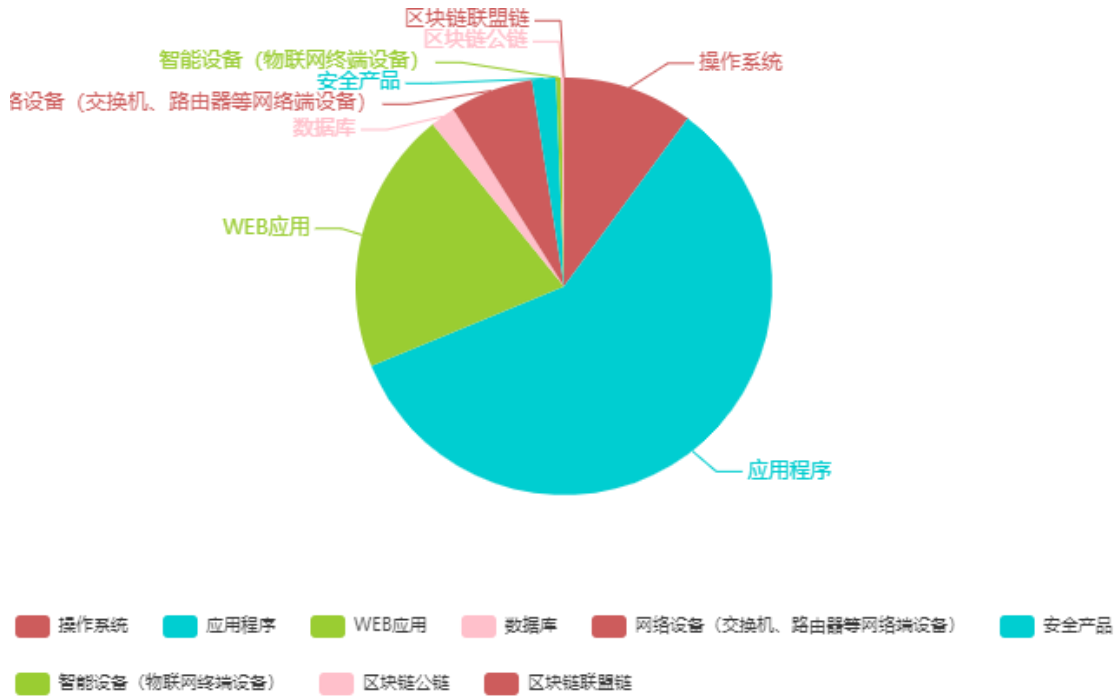
➢ 漏洞产生原因（2020 年 06 月 07 日—2020 年 06 月 21）



➢ 漏洞引发的威胁（2020 年 06 月 07 日—2020 年 06 月 21）



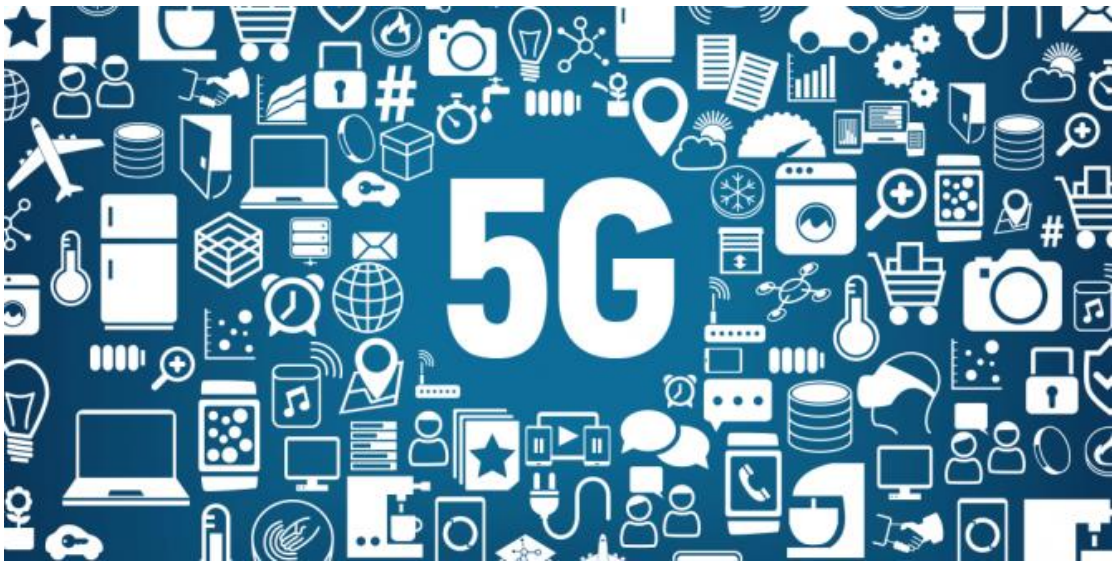
➢ 漏洞影响对象类型（2020 年 06 月 07 日—2020 年 06 月 21）



三、安全产业动态

➢ 推进新基建信息安全也得跟得上

在我们的日常生活中，许多人都遇到过这样的情况：在某些搜索引擎上对自己感兴趣的内容进行搜索阅读后，打开购物软件却收到与刚刚阅读内容相关的推送……前脚进行了一些与培训相关的咨询，后脚就有可能收到课程推介的电话……这样看似“神操作”的背后，是令人深思的数据安全与信息安全问题。



安全问题在互联网领域早已是老生常谈的问题，随着数字经济不断发展，5G 等新型基础设施建设的加快推进，5G + 大数据、5G + 云计算等应用层出不穷。北京邮电大学曾剑秋教授曾指出，随着 5G 的发展，用户产生的数据不断增加，企业拥有的用户信息也不断增加。例如，今日头条、快手等 App 会根据用户平时显示的喜好向用户推荐新的内容。此外，5G 可以释放智慧城市的力量，其中城市中的物联网设备将会识别用户的语音、面部表情和手势等，并将它们转换成可选择按钮，这样的 5G + 大数据应用会给我们的生活和工作带来更多的便利和更多的产品与服务，但是隐私泄露问题也成为人们抱怨的焦点。“用户第一次注册或登录 App 时，都会询问用户是否授权 App 获取地理位置、访问手机联系人、识别手机标识、访问麦克风和摄像头等。有些授权被用户拒绝不影响软件使用，然而，一些情况是授权如被拒绝，软件会自行退出或提醒用户不可拒绝。这种情况下，如果用户想要使用产品就必须选择同意，但这也意味着自己的部分信息或隐私被软件获取。大数据使信息获取更容易、更透明、更智能的同时，也带来了隐私泄露问题。曾剑秋认为，大数据在传统行业应用的过

程中，产生了规模更加庞大的数据，也对数据的时效性与传输速率提出了更高要求，5G 技术能满足大数据产业对于海量数据传输、存储、处理的需求，其可能存在的数据安全问题主要涉及几个方面。

首先是 5G 技术的核心网和边缘网络数据安全问题。“核心网是通信网络的大脑，负责对整个网络进行控制和处理；边缘网络指的是核心网络与企业、学校等用户之间连接的网络。这些基础设施一旦被入侵，将可能产生网络连接中断、重要数据被窃取等问题，导致数据安全受到威胁。”

其次，5G 网络凭借其大带宽、低时延以及高可靠的特点衍生出很多新的应用场景。曾剑秋表示，以高清视频为例，不同的场景使得数据安全的边界比以往更为模糊。“哪些数据可以收集，哪些数据不能收集，这些在场景应用过程中都是需要认真思考的。同时，这也是 5G + 大数据应用可能产生数据安全问题的新特点。”

再次，5G 网络实现万物互联可能产生数据安全问题。5G 到来以前，人们使用网络还主要以人与人的数据连接为主，5G 时代，人与人之间连接更加紧密，而且人与物、物与物之间也彼此相连。在这样的环境下，一些低成本网络连接设备有可能成为比较容易被攻击的对象，黑客就可能会控制住这些脆弱的网络连接设备，然后从后台下载企业和用户的信息，导致信息泄露、数据信息不安全。

最后，数据安全意识薄弱带来的隐私泄露、数据信息不安全问题。“5G + 大数据的到来也让一些企业措手不及，一些企业对数据安全、网络安全不重视，企业的数据库常年‘裸奔’，很容易被攻击。与此同时，5G + 大数据使企业办公网络的边界不再固定，通过公司内网、无线网、移动互联网等接入办公网络越来越多，员工在家远程工作会越来越常态化。但是，我们的安全保障措施在哪里？这也是值得深思的问题。”曾剑秋说道。

针对技术发展带来的信息安全问题，中国政法大学传播法研究中心的朱巍教授也表示出一些担忧。朱巍认为，尽管隐私权本质属于民事权利，如果平台事先充分告知用户收集数据的范围、类型和目的，按照合法性、正当性和必要性的基本原则依法使用，一般来说，平台是可以通过网民协议等方式处理用户数据信息的。然而，移动端作为网络支付和社交平台，人脸识别就好比能够打开用户家大门的钥匙。“网民协议作为君子协议，平台好好遵守倒是无妨，一旦发生了信息泄露或使用不当，这个危害是非常大的，数据的可复制性将注定事后处置不能完全去除危害。”

5G 时代数据安全、信息安全想要得到有效保护，国家层面的法律制定必不可少。今年全国两会上，一个重要信号得以释放：全国人大常委会工作报告在下一步主要工作安排中指

出，围绕国家安全和社会治理，制定个人信息保护法、数据安全法。此前，新华社曾发布消息，从全国人大常委会法工委获悉，个人信息保护法正在研究起草中，草案稿已经形成。个人信息保护法、数据安全法的出台将为 5G 时代下数据信息的安全使用提供有效支撑。

然而，光依赖法律并不足以保证数据与信息的安全。曾剑秋认为，5G + 大数据的数据安全保护首先在于国家构建的网络安全保障体系和一系列的政策措施。网络安全是国家安全，企业和个人的数据安全是国家安全的重要组成部分，手机用户实行实名制、互联网如微信后台必须实名，5G + 大数据技术对数据信息的反应速度以及对 IP 地址的处理能力的大幅度提升，为减少隐私泄露、保护数据信息安全奠定了坚实的基础，形成了可靠的保护伞。5G + 大数据使边缘计算迅速崛起，是数据信息安全保护的新神器。边缘计算就是将大量的数据分析功能从数据中心下沉到更靠近应用的地方，从而大大缓解计算中心的压力，既可以有效减小计算系统的延迟，提高可用性，又能够有效保护数据安全和隐私。互联网数据中心报告数据显示，5G 时代将有 45%的物联网数据通过边缘计算进行存储、处理和分析，以此提高数据中心的工作效率和数据信息的保护程度。5G 为每一个 5G 手机用户设置了唯一永久标识，以确定手机用户的真实身份，并保护用户在网络上传输的数据安全。5G 还可以通过设置公钥、私钥体系对用户在网络上传输的数据进行加密处理。公钥是公开的，终端用户用来加密数据；私钥是保密的，用以解密、保护用户的数据安全。如此一来，攻击者即使劫持了用户的信息，只有公钥，没有私钥，也无法盗取用户隐私数据。“数据信息、隐私保护首先是一个个体的事情，各个环节、各个企业、每个人均需要有数据信息安全和隐私保护的意识，例如，不要随意授权 App 获取自己的数据，维护自身的数据安全。”（来源：人民邮电报）

➢ 2020 版《个人信息安全规范》你不得不重视的第三方接入管理规则

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”）。在新标准中，我们留意到了一个非常可喜的变化，即在个人信息的委托处理、共享、转让、公开披露方面，新增了关于“第三方接入管理”的详细规定，包括了要求进行安全评估、明确安全责任、需要告知个人信息主体等。在现今 APP 大量使用到第三方接入程序/软件（例如 SDK 包），并可能由于这些第三方接入程序/软件过渡索权、

超范围收集个人信息等问题日益严重的今天，新标准进一步明确了个人信息控制者对第三方接入管理的要求，是一个非常重要的环节，也是规范技术进步的很好体现。

1、如何正确理解“第三方接入？”

相关法律中暂无对“第三方接入”的定义。这里说的第三方接入，主要是互联网产品或服务的过程中，接入了第三方的产品或服务，具体到应用场景而言的话，比如说某应用程序或网页接入了第三方的软件工具开发包 SDK，或调用了第三方的 API 接口等。特别地，当这个被接入的第三方产品或服务具有收集个人信息的功能时，需要向个人信息主体明确告知，征得个人信息主体的明示同意，接受新标准关于“第三方接入管理”的相关规定。这一点，与信安标委于 2020 年 3 月 30 日新发布的《移动互联网应用程序（App）个人信息安全防范指引（征求意见稿）》（“安全防范指引”）的规定也互相呼应，当中也要求了需要对嵌入的收集用户个人信息的第三方 SDK 进行披露，告知第三方 SDK 类型，及收集使用的个人信息的目的、方式和范围。特别在涉及敏感信息时，还需要告知接收方的身份和数据安全能力，并征得明示同意，当用户撤回同意后，还需要帮助用户删除在第三方 SDK 的相关数据。

其实，以移动应用程序的业务场景为例，一个 APP 开发并没有想象中那么容易，表面看起来很简单的功能，背后实际由各种复杂的技术在支撑。很多情况下，考虑到快速上线以及整体预算的控制，APP 的开发者或运营者常常会借助第三方技术服务的力量，帮助产品实现功能并提供更多样的服务，这时，就出现了大量接入第三方产品和服务的场景了。以常见的

视频直播 App 为例，在支付提现、分享、定位、云存储、加速服务等功能实现过程中均涉及到接入或使用第三方服务。

2、为什么需要重视对“第三方接入”进行管理？

为了能更好地理解对第三方接入管理的重要性，我们以最容易产生个人信息安全风险的第三方 SDK 为例进行说明。

SDK 是第三方接入的典型例子，先来看看什么是 SDK。SDK 即软件开发工具包（Software Development Kit），是软件工程师用于为特定软件包、软件框架、硬件平台、作业系统等创建应用软件的开发工具集合，开发者无需了解 SDK 内部实现细节，只需要调用程序接口，便可以帮助 App 实现登陆分享、支付、广告、数据统计、地图、风控插件等一系列功能。为了审视 SDK 相关的安全问题，根据使用形态对 SDK 进行分类，可以分为：（1）引入 SDK: 自身应用中集成引入的第三方 SDK（例如 ZOOM 事件中内嵌了脸书的 SDK）；（2）外发 SDK：将自身业务服务封装，发布出去给第三方厂商调用使用的 SDK。

这些第三方 SDK 有着各类神通广大的功能，比如，专业型的 SDK 根据功能的不同可以实现推送、通信、存储、安全、地图及位置服务、统计及增长、社交、广告、语音识别、图像识别等各种功能（例如金融行业的开放银行领域，银行业者通过将自己的业务服务和数据服务封装到一个 SDK 中，实现向第三方合作伙伴提供开放金融能力）。

我们以通过 Android 提供的标准系统加入平台获取为例，SDK 可以收集的信息包括：

（1）应用信息类：到用户手机上已经安装的 App 信息列表和正在运行的应用列表；

（2）账号信息类：用户账号信息；

（3）网络相关信息类：用户移动设备的联网信息、用户通信的设备信息、GPS、NFC 信息等；

（4）设备信息类：用户移动设备标识信息、手机 IMEI 码、SIM 标识信息等；

（5）传感器信息类：不同型号的移动设备，集成传感器的数量与种类也有所区别，比如用户的行踪可以通过位置传感器精确追踪。

第三方接入存在的安全隐患及可能引发的个人信息安全问题包括：

（1）隐瞒收集个人信息的情况

当第三方接入的产品或服务（例如 SDK）一样具有收集用户个人信息的能力的时候，在较多的情况下，用户较难感知，甚至 App 的运营者或开发者也未必都知道这些第三方接入的产品收集了哪些个人信息。一旦这些第三方接入的产品在没有经过用户同意的情况下，收集了各类与用户密切相关的敏感信息（例如银行账号，生物特征信息等），并传输到其他服

务器甚至境外，将会引发极大的个人数据隐私风险。

（2）程序自身存在安全漏洞

以第三方 SDK 为例，目前，已经发现的 SDK 安全漏洞包括 HTTP 误用，SSL/TLS 不正确配置、敏感权限滥用、通过日志造成信息泄露等。如果一个 App 嵌入的第三方 SDK 越多，它的安全漏洞可能就越明显，影响范围也就越大。

（3）违反个人信息收集的“最小使用”和“目的限制”原则

标准明确了个人信息安全的七项基本原则，其中“最小必要原则”是指，只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时删除个人信息。而“目的明确原则”则是指，需要具有明确、清晰、具体的个人信息处理目的。但是很多第三接入的产品或服务经常通过不透明的方式，大量高频次地收集用户的个人信息，而往往这些被收集的个人信息与业务功能并没有任何直接或间接的关联。

（4）恶意第三方接入（例如 SDK）导致软件供应链污染

比如说，“引入 SDK”的主要安全风险来自 SDK 自身的恶意行为。由于 Android 操作系统带有热更新机制，这使得一部分恶意 SDK 在客户集成阶段会表现为一个非常正常的应用，而一旦应用发布后到了运行阶段，攻击者就会通过热更新机制，更新恶意代码，执行盗取用户数据、采集敏感信息等恶意行为。这种发布后作恶的行为在很大程度上绕过了发布前的静态检测，具有非常大的迷惑性，也使得其作恶行为更加难以被发现。而“外发 SDK”的风险则主要存在于在发布后的运行阶段，极容易遭遇剥离、破解、注入、调试和渗透测试等运行时攻击行为。

3、存在“第三方接入”情形时，如何分辨场景、角色和责任？

当个人信息控制者在其产品或服务中接入具备收集个人信息功能的第三方产品或服务时，个人信息控制者和第三方接入服务或产品供应商在数据收集、使用的环境中，将会由于不同的合作关系或个人信息处理活动，而处于个人信息控制者、共同控制者或者接受控制者委托的信息处理者地位，需要进行具体的分析。下面，我们将结合新标准的规定，根据不同的情况，进行分析。

（1）当第三方接入的产品是接受网站经营者的委托而进行处理个人信息时，网站经营者（例如：宿主 APP）接入了第三方的产品，并委托第三方对个人信息进行处理，网站经营者对个人信息处理的目的和范围决定，受托的第三方接入产品应按照网站经营者的指示进行处理个人信息。那么，网站经营者属于个人控制者，接入的第三方仅构成个人信息处理者。例如 APP 运营者在应用程序中部署了第三方统计分析类的 SDK，第三方完全按照宿主 APP

的指示将个人信息用于统计分析，不能将个人信息再与第三方共享或超出授权委托处理的范围。

（2）当第三方接入的产品与网站经营者共同处理个人信息时，网站经营者与第三方共同决定了个人信息处理的范围和目的，此时，第三方可能构成个人信息共同控制者。例如在宿主 APP 中嵌入了第三方支付 SDK 或调用了第三方地图供应商的 API 接口，第三方对数据使用目的、使用方式也享用了共同决定权，与宿主 APP 一起决定第三方 SDK 收集哪些信息等。此时，特别需要注意的是，新标准以及上述提及的“安全防范指引”都明确要求了网站经营者需要向用户明确告知第三方收集个人信息的情况并取得用户同意。特别地，当接入的第三方服务仅提供或支持扩展业务功能时，还要求就第三方提供的扩展业务功能进行逐项说明并取得用户明示同意（新标准提高了对扩展业务功能的告知和同意要求）。

关于此点，在新标准中的 9.6 条，也明确表示了，当个人信息控制者在提供产品或服务的过程中部署了收集个人信息的第三方插件（例如，网站经营者与在其网页或应用程序中部署统计分析工具、软件开发工具包 SDK、调用地图 API 接口），且该第三方并未单独向个人信息主体征得收集个人信息的授权同意，则个人信息控制者与该第三方在个人信息收集阶段为共同个人信息控制者。

新标准通过上述这些要求，进一步地应对了第三方接入的常见问题，例如网络经营者没有向用户告知第三方接入的产品收集了哪些信息，没有取得用户的同意，在第三方接入的产品超出授权范围收集个人信息或变更使用目的时只是获得用户的概括式授权同意等问题。关于以上第 1 点和第 2 点的情况，按照新标准的规定，如果该第三方构成接受控制者委托的信息处理者或者为共同控制者，适用标准第 9.1（委托处理）和 9.6（共同个人信息控制者）的规定。

（3）当网站经营者接入或跳转到第三方接入的产品时，第三方通常对个人信息处理的范围和目的享有决定权。例如当一些直接收集类的 SDK，可以在即便宿主 APP 关闭了部分权限的情况下，也可以通过一些绕过的手段收集用户的个人信息。此时，第三方接入是为了获得个人信息并且实现该第三方提供的服务功能，因此第三方不是接受委托处理个人信息的受托方，同时，如果宿主 APP 并不控制这些收集的数据，而是由第三方接入的这个产品实际控制了这些收集的数据，第三方接入很可能成为个人信息的控制者。例如视频直播软件接入了第三方的支付 SDK 的情况。

但实践中多数情况下，网站经营者（例如宿主 APP）通常并没有清晰地明确这些服务是由哪些第三方提供的，第三方接入都收集了哪些信息，也没有对第三方接入提供的服务进行

明确的区分，更没有对第三方接入的产品或服务进行有效的技术审查和监督管理，从而导致各类安全漏洞，引发严重的个人信息安全风险。因此，新标准特别就这一点进行了详细的明确。

4、“第三方接入”情境下落实标准要求的建议

从新标准的规定可以看出，关于对第三方接入的管理，与共享、转让、委托处理中的规定和责任相似，例如，包括在事前建立第三方产品或服务接入管理机制，在接入后对第三方产品和服务进行持续监督、通过签署合同约束双方责任、需要明确告知个人信息主体服务由第三方提供、对记录进行保存、要求第三方确保个人信息主体授权同意、对第三方接入的自动化工具技术进行技术检测等等。具体建议如下：

（1）建立管理机制：建立第三方产品或服务接入管理机制和工作流程，必要时应建立安全评估等机制设置接入条件。例如，审慎接入第三方 SDK，具体要审核第三方 SDK 的代码是否安全、收集了哪些信息、采取了哪些安全措施、在哪里存储、具体的使用方式、使用内容、权限申请等。

（2）签署合同：应与第三方产品或服务提供者通过合同等形式明确双方的安全责任及应实施的个人信息安全措施。

（3）明确标识：应向个人信息主体明确标识产品或服务由第三方提供。例如，当接入了具备收集个人信息的产品或服务时，需要在隐私政策中明确披露接入的第三方 SDK 的名称、接入目的、收集和使用范围等。

（4）明示具体功能：如果通过嵌入第三方代码、插件等方式将个人信息传输至第三方服务器，应通过弹窗提示等方式明确告知用户。

（5）保存记录：应妥善留存平台第三方接入有关合同和管理记录，确保可供相关方查阅。

（6）要求第三方获得授权同意：应要求第三方根据本标准相关要求向个人信息主体征得收集个人信息的授权同意，必要时核验其实现的方式。

（7）要求第三方建立响应机制：应要求第三方产品或服务建立响应个人信息主体请求和投诉等的机制，以供个人信息主体查询、使用。

（8）监督管理：应监督第三方产品或服务提供者加强个人信息安全管理，发现第三方产品或服务没有落实安全管理要求和责任的，应及时督促整改，必要时停止接入。

（9）技术检测：当产品或服务嵌入或接入第三方自动化工具（如代码、脚本、接口、算法模型、 软件开发工具包、小程序等）时，开展技术检测确保其个人信息收集、使用行

为符合约定要求。

（10）进行审计：对第三方嵌入或接入的自动化工具收集个人信息的行为进行审计，发现超 出约定的行为，及时切断接入。

结语：新标准对第三方接入管理提出了更高的要求，特别是对第三方 SDK 的监管，也很可能成为本年度的监管重点之一。这也意味着，对于网络经营者而言，也将承担更大的个人信息保护责任，并采取措施落实各项要求，包括需要对接入的第三方进行评估审查，对用户告知和同意机制进行完善，还需要与第三方接入供应商签订合作协等，企业或平台能否有足够的能力或资源完成这些要求，以及这些监督义务需要履行到何种程度适宜，将值得司法界、学术界、企业界等全行业一起继续探讨。（来源：全国信息安全标准化技术委员会）

➢ 《网络安全审查办法》的审查体系与实施影响分析

2020 年 4 月 27 日，在历时两年多试行基础上，《网络安全审查办法》（以下简称“《办法》”） 正式发布，《网络产品和服务安全审查办法（试行）》（以下简称“《试行》”）同时废止，体现出网络安全审查制度两年多来的演化痕迹和经验沉积。《办法》整体上更加聚焦于国家安全和关键信息基础设施保护，是落实“着力提升关键信息基础设施安全防护水平”的有力举措。在国际形势日益复杂，国家间政治、经济、技术博弈日益激烈的背景下，《办法》的出台对国家安全乃至国际关系都将产生深远影响。分析《办法》的监管模式、审查主体、审查原则、考虑因素、审查流程和具体实施影响，有助于厘清权责，推动制度落地。

一、网络安全审查的法律定性与协调监管模式

《办法》明确立法目的在于确保关键信息基础设施供应链安全，维护国家安全，并由 12 个部门共同制定、联合发布，从意旨和阵容上都给出了《办法》的网络安全审查法律定性，即为《国家安全法》第五十九条规定的“网络信息技术产品和服务”审查（国家安全审查）和《网络安全法》第三十五条规定的“网络产品和服务” 审查（网络安全审查）。

网络安全审查是国家安全审查的重要内容，为国之利器，既要周延地论证审查范围，明确实施审查的机构；也需审慎考察审查程序，特别是触发审查的条件。《办法》确立了 12 个部门联席审查工作机制，构建了网络安全审查办公室、网络安全审查工作机制成员单位、相关关键信息基础设施保护工作部门共同参与的网络安全多重审查架构，并赋予中央网络安全和信息化委员会特别审查个案的最终决策权，我国网络安全审查的协调监管模式正式确立。

网络安全审查办公室承担第一重审查职责，《办法》明确“网络安全审查办公室设在国家互联网信息办公室，负责制定网络安全审查相关制度规范，组织网络安全审查”。按照国家互联网信息办公室有关负责人答记者问的表述：“具体工作委托中国网络安全审查技术与认证中心（以下简称“认证中心”）承担。认证中心在网络安全审查办公室的指导下，承担接收申报材料、对申报材料进行形式审查、具体组织审查工作等任务”，考虑到认证中心本身应具有的专业性，《试行》第十一条规定的“网络安全审查第三方机构”终于落定。

二、申报决策的角色转变与未来应关注的审查领域

《试行》第二条规定 “关系国家安全的网络和信息系统采购的重要网络产品和服务，应当经过网络安全审查”，“关键信息基础设施运营者采购的网络产品和服务，可能影响国家安全的，应当通过网络安全审查”，而对于是否影响国家安全的认定，规定“由关键信息基础设施保护工作部门确定”。这种规定存在“下位法规定任意扩大网络安全审查范围”的问题，曾引起了广泛争议。

《试行》赋予关键信息基础设施保护工作部门审查网络安全审查申报者的权力，事实上不仅使关键信息基础设施运营者产生决策依赖，影响其申报意愿和能力，还可能形成不同行业、领域衡量和评价尺度不一的“壁垒”，无法实现审查涉及领域的“适配性”和“均衡化”。

针对这一关键问题，《办法》规定，“关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，应当按照本办法进行网络安全审查”，即由关键信息基础设施运营者自行判定采购行为和供应链安全，在此基础上启动网络安全审查。将关键信息基础设施保护工作部门的作用内化为制定本行业、本领域的网络安全审查预判指南，从决策向指引角色转变。

根据中央网络安全和信息化委员会《关于关键信息基础设施安全保护工作有关事项的通知》的精神，电信、广播电视、能源、金融、公路水路运输、铁路、民航、邮政、水利、应急管理、卫生健康、社会保障、国防科技工业等行业领域的重要网络和信息系统运营者在采购网络产品和服务时，应当按照《办法》要求考虑申报网络安全审查。

关键信息基础设施安全保护制度建设已全面铺开，2017 年 7 月 11 日国家互联网信息办公室发布《关键信息基础设施安全保护条例（征求意见稿）》，经过近 3 年的时间，保护条例进入立法实质性阶段。在保护条例所确立的具体识别或者认定方法正式发布之前（是否以识别或认定方式发布指引尚存在不确定性），网络运营者可以参照前述通知衡量其是否属于关键信息基础设施，从而判定是否需要进行网络安全审查。

三、审查原则与考虑因素

《试行》规定，网络安全审查的原则为“坚持企业承诺与社会监督相结合，第三方评价与政府监管相结合，实验室检测、现场检查、在线监测、背景调查相结合，对网络产品和服务及其提供者进行网络安全审查”，《办法》进一步明确为“网络安全审查坚持防范网络安全风险与促进先进技术应用相结合、过程公正透明与知识产权保护相结合、事前审查与持续监管相结合、企业承诺与社会监督相结合，从产品和服务安全性、可能带来的国家安全风险等方面进行审查”，将安全与发展的关系、透明度、中立性、持续性作出适当延展，同时不再对实验室检测、现场检查、在线监测、背景调查等实际上属于具体的审查方式进行规定。

从整体上，这些原则显得更像“原则”，因此未来实际审查牵涉的方面和手段也会比《试行》更为庞杂和丰富。实际上无论是审查原则、启动触发条件或是审查过程，都对申报者的“理解能力”提出了更高要求。

根据这些原则，《办法》对《试行》中的不合理条款进行了剔除，例如第十条等，并强化了对包括运营者、产品和服务提供者在内的各方商业秘密等知识产权的保护，包括对于审查结论，《办法》规定为“通知运营者”而不再是随意性的“发布”，也契合了上述保护意识，一并构成了《办法》的重要原则。顺带提及的是，《办法》第十六条规定，“参与网络安全审查的相关机构和人员应严格保护企业商业秘密和知识产权”，这里将商业秘密和知识产权并列的表述缺乏严谨性。

对于审查考虑的实质性因素，尽管其是作为网络安全审查的流程中评估国家安全风险的要素进行的规定，但实际上构成了各方最为关注的“触发和评价是否危害国家安全的网络安全审查的条件”参照。《办法》将《试行》的若干审查要素重新进行了梳理，《试行》第四条第（一）项和第（三）项整合纳入《办法》第九条的第（一）项，《试行》第四条第（二）

项和第（四）项重新表述为《办法》第九条的第（三）项，整体而言，表述更为凝练和“委婉”。

本文认为，《办法》的第九条第（二）项可以理解为产品和服务的直接供应中断，通常而言是产品和服务提供者（供应商）自身“技术原因导致的供应中断”，而第（三）项则强调了外部非供应商自身技术能力导致的供应中断风险，这些风险的不确定性评估实际上超出了运营者和供应商的认知。如增加考虑第（四）项供应商对中国法律的合规性情况，则会进一步加剧供应商的担忧。

此外，考虑因素中的某些表述未来有待于更加明确的解释，例如“开放性”与“透明性”的区分和解释。如果后者指向源码访问或审查，前者的含义怎么界定。而“来源的多样性”，在关键信息基础设施运营者公开程序（例如招标）中，尚未实际采购产品和服务时如何实际操作，即在未采购时作为招标条件本身即不限定（也不应限定）来源，而在招标程序后则意味着来源确定，这些都有待观察。

四、运营者主动申报和依职权启动审查的流程

对于审查流程的程序性考察，《办法》首先排除了《试行》第九条规定带来的困惑，明确了申报流程和主要步骤包括：

（1）申报者在采购网络产品和服务之前进行国家安全风险预判；

（2）经预判可能影响国家安全的，向网络安全审查办公室（通过认证中心）申报网络安全审查；

（3）同时，申报者可通知产品和服务提供者配合审查；

（4）提交材料，申报网络安全审查；

（5）10 个工作日内完成确定，属于需要审查的，书面通知运营者；

（6）30 个工作日内完成初步审查（情况复杂的，可以延长 15 个工作日），并形成审查结论建议，将审查结论建议发送网络安全审查工作机制成员单位、相关关键信息基础设施保护工作部门征求意见；

（7）网络安全审查工作机制成员单位和相关关键信息基础设施保护工作部门应当自收到审查结论建议之日起，在 15 个工作日内书面回复意见，将审查结论通知运营者；

（8）如两者意见不一致，进入特别审查程序，最终经报中央网络安全和信息化委员会批准，形成审查结论并书面通知运营者。特别审查程序一般应当在 45 个工作日内完成，情况复杂的可以适当延长。

除运营者作为申报者启动审查申报之外，《办法》还规定“网络安全审查工作机制成员

单位认为影响或可能影响国家安全的网络产品和服务，由网络安全审查办公室按程序报中央网络安全和信息化委员会批准后，依照本办法的规定进行审查”，即网络安全审查工作机制成员单位可主动申请对特定网络产品、服务适用网络安全审查。

较《试行》规定“国家有关部门要求、全国性行业协会建议、市场反映和企业申请”的宽泛表述，更为聚焦。依职权主动启动审查程序，将会对运营者和供应商的权利义务造成重大影响，因此《办法》规定的“由网络安全审查办公室按程序报中央网络安全和信息化委员会批准后”，方能进行审查，显示了网络安全审查启动程序的审慎，契合了立法目的。

五、合规风险问题

鉴于利益相关方对网络安全审查制度的不同理解，《办法》的实施效力有待未来实践检验。对于网络安全审查的考虑因素，未来是保持国家安全审查的适当封闭性，还是可能按照《认证认可条例》等法律法规的要求，进行认证中心认证规制的适当标准化，尚有待进一步观察。但毫无疑问的是，认证中心将开始新的职责转变或相关业务剥离等处理，确保网络安全审查实施的中立性和独立性。例如，是否考虑对“受理认证委托、实施评价、做出认证决定，颁发认证证书”等现有职责进行调整，避免对某些产品、服务进行认证的同时又对采购该产品、服务的网络安全风险进行网络安全审查。

在运营者之外，《办法》对产品、服务提供者增加和转移的隐性义务规定也将导致供应链关系的深刻变化，运营者和供应商都应结合适用性与否的基本判断，进一步评估《办法》带来的成本、投入与合规风险。

此外，按照《办法》及其答记者问精神来看，运营者应当在与产品和服务提供方正式签署合同前申报网络安全审查。如果在签署合同后申报网络安全审查，建议在合同中注明此合同须在产品和服务采购通过网络安全审查后方可生效，以避免因为没有通过网络安全审查而造成损失。

对于这里的将“产品和服务采购通过网络安全审查”是否可以作为合同生效要件的疑问，本文认为，采购合同中各方可以分别约定合同成立和生效要件。如运营者未进行类似生效要件规定的，则未来在发生法律争议或损失时，将很难以“需经过网络安全审查”为由主张合同无效，因此这一条款尤为必要。

六、结语

关键信息基础设施安全保护是关乎国家战略的优先事项，也是我国整体网络安全保障工作的重中之重。网络安全审查制度通过识别可能的安全风险，从源头上防范、缓解、控制可能影响关键信息基础设施供应链正常运行的潜在威胁，是维护国家安全、网络安全的重要举

措和关键手段。

《办法》较之《试行》，规定了更为科学的审查原则、协调监管模式、更加合理的审查启动和审核程序，审查重点明确清晰，增加了该项制度的可操作性，为关键信息基础设施的安全持续、稳定运转构筑了有效框架，具有现实意义。

未来几年，《办法》的实施将逐步展开，监管机构应该继续推动并完善各项规定，促使网络安全审查制度全面落地。（来源：《信息安全与通信保密》2020 年第六期）

➢ 民法典保障个人信息安全可控

我们生活所处的社会一直在随着科学技术的发展而发生变化，民法以保护民事主体的合法权益、维护社会和经济秩序为根本目标，通过赋予个体以民事权益而确保我们在享有科技便利的同时也拥有安全可控的生存环境。

马克思曾经深刻的指出：法律应该以社会为基础。第二次工业革命（特别是新闻出版业的繁荣）催生了隐私权的概念，第三次工业革命（特别是计算机的应用）激发了个人信息保护的需求，而新一代信息技术和数字经济的发展则使得个人信息安全可控成为必然的趋势。《中华人民共和国民法典》是中国特色社会主义法律体系基本形成之后唯一以“法典”命名的立法，是中国民事立法和司法实践成就的一次总结，同时也结合新的社会发展形势发展了新规则，在总则以及“人格权编”第六章规定了隐私权和个人信息保护的要求，体现了信息时代的民法发展趋势。

一、比隐私权更广泛的个人信息保护

因为信息技术的全面普及，互联网成为社会交往的纽带，数字化转型成为经济发展的新动力，我们每个人都在网络空间具有了数字化身份，通过我们在网络空间的活动留下了许多记载我们社交关系、活动轨迹等等的数字脚印。当我们在享受数字化服务、在数字化场景活动以及接受信息化管理的过程中，都不可避免的要输入和产生许多类型的个人信息。

2009 年颁布的侵权责任法已经确立了“隐私权”是受法律保护的民事权利，此次民法典第一千零三十二条则进一步明确：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。隐私权的价值就是维护我国宪法所规定赋予公民的人格尊严、住宅、通信自由，是一项具有绝对性和支配性的独立民事权利。然而，那些接受管理、服务过程中由个人主动告知的个人基本资料、个人财产信息、个人健康生理信息、个人上网记录，对于信息的处理者和控制者而言并不属于私密信息，故而无法受到隐私权的保护。

个人信息可以被各种形式收集，并被用于商业服务和社会管理的各个领域。为了保护我们的个人信息安全，民法典在总则部分的第一百一十一条规定：自然人的个人信息受法律保护。任何组织或者个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。民法典还专章规定了“隐私权和个人信息保护”，进一步表明我们在隐私权之外需要的更多的信息安全。

个人信息本身是信息社会中频繁使用和产生的内容，为何其保护价值依然重要，主要是因为个人信息承载了人身权和财产权的安全，个人信息的安全是保障我们人身权和财产权安全的基础。

二、维护个人对其信息的控制权

我们的日常工作和生活中需要大量的使用个人信息，但是这并不意味着个人信息成为任何单位和个人自由掠夺的资源。维护个人对其信息的控制权是民法典新增个人信息保护条款的主要目标，这种控制权包括控制个人信息的流出，更正或撤回个人信息的存储与使用，维护个人信息的安全环境。

知情同意是控制个人信息流出的关键措施。根据民法典第一千零三十五条的规定，处理自然人个人信息的，一般都必须征得该自然人或者其监护人同意，否则不得收集、存储、使用、加工、传输、提供、公开个人的信息。即便是获得了个人的同意，在处理个人信息过程中还需要明示处理信息的目的、方式和范围，不违反法律、行政法规的规定和双方的约定，并按照合理的方式公开处理信息。

查询、复制并行使删除权是确保个人信息主体控制权的具体措施。根据民法典第一千零三十七条的规定，自然人可以依法向信息处理者查阅或者复制其个人信息；发现信息有错误的，有权提出异议并请求及时采取更正等必要措施。与此同时，自然人发现信息处理者违反法律、行政法规的规定或者双方的约定处理其个人信息的，有权请求信息处理者及时删除。通过这些具体措施的赋权，个人可以掌控其个人信息的使用状态，并且对相关的状态进行调整，乃至是提出删除的要求，个人信息的处理者都需要满足上述个人权利主张。

对信息处理者施加必要的安全保障责任是维护个人信息控制权的必要措施。根据民法典第一千零三十八条的规定，信息处理者不得泄露或者篡改其收集、存储的个人信息；未经自然人同意，不得向他人非法提供其个人信息。信息处理者应当采取技术措施和其他必要措施，确保其收集、存储的个人信息安全，防止信息泄露、篡改、丢失；发生或者可能发生个人信息泄露、篡改、丢失的，应当及时采取补救措施，按照规定告知自然人并向有关主管部门报告。由于政府掌握了最大量最重要的个人信息，民法典第一千零三十九条特别强调，国家机关及其工作人员对于履行职责过程中知悉的自然人的隐私和个人信息，应当予以保密，不得泄露或者向他人非法提供。

由于个人信息的利用对新一代信息技术的发展和公共利益的维护也具有重要意义，所以民法典在安全可控的情况下也为个人信息合理使用提供了必要的空间。民法典第一千零三十六条特别列举了三种合理使用的情况，分别为（1）在该自然人或者其监护人同意的范围内合理实施的行为；（2）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；（3）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。这些举措为科技企业提供数字化产品或服务创造了使用个人信息，为政府在新冠肺炎疫情管控等管控措施中依赖个人信息实现治理体系和治理能力现代化，还为利用公开的个人信息开展社会交流、科学研究和自由表达，均提供了合法的条件和依据。

全国人民代表大会常务委员会副委员长王晨向第十三届全国人民代表大会第三次会议作“关于《中华人民共和国民法典（草案）》的说明”中，特别指出：第四编第六章是在现行有关法律规定的基础上，进一步强化对隐私权和个人信息的保护，并为下一步制定个人信息保护法留下空间。随着民法典的颁布和个人信息保护法的制定，将共同为我们创造一个更加安全可控的信息化生存环境，同时也将促进消费者更加信任数字化技术所带来的积极作用，实现科技发展与个体安全的双重目标。（来源：法制日报）

四、政府之声

➢ 国家版权局等四部门启动“剑网 2020”专项行动

2020 年 6 月 12 日，国家版权局、工业和信息化部、公安部、国家互联网信息办公室四部门联合启动打击网络侵权盗版“剑网 2020”专项行动，这是全国持续开展的第 16 次打击网络侵权盗版专项行动。自 2005 年起，国家版权局等部门针对网络侵权盗版的热点难点问题，先后开展了网络视频、音乐、文学、新闻及网络云存储空间、应用程序商店等领域的版权专项整治，集中强化对网络侵权盗版行为的打击力度，相继查处了一批侵权盗版大案要案，有效打击和震慑了网络侵权盗版行为，改变了网络视频、网络音乐、网络文学等领域版权秩序混乱的局面，得到国内外权利人的充分肯定。

本次专项行动于 6 月至 10 月开展，针对网络版权保护面临的新情况新问题，聚焦 5 个重点领域：一是开展视听作品版权专项整治，深入开展院线电影网络版权专项保护，严厉打击短视频领域存在的侵权盗版行为，严厉打击通过流媒体软硬件传播侵权盗版作品行为；二是开展电商平台版权专项整治，加强对大型电商平台的版权监管工作，严厉打击网店销售盗版图书、音像制品、电子出版物、数据库及盗版网络链接和存储盗版作品的网盘账号密码等行为，严厉整治网店设计、经营中使用盗版图片、音乐、视频等行为；三是开展社交平台版权专项整治，加大新闻作品版权保护力度，进一步规范图片市场版权传播秩序，关闭一批恶意侵权社交平台账号；四是开展在线教育版权专项整治，加大“学习强国”学习平台版权保

护力度，大力整治在线教育培训中存在的侵权盗版乱象，切断盗版网课的灰色产业链条；五是巩固重点领域版权治理成果，严厉打击网络游戏私服、外挂等侵权盗版行为，推动完善网络音乐版权授权体系，强化对大型知识分享平台的版权监管力度，继续巩固网络文学、动漫、网盘、应用市场、网络广告联盟等领域取得的工作成果。

国家版权局有关负责人表示，本次专项行动将突出查办案件，进一步加大对网络侵权盗版案件的处罚力度，对人民群众意见强烈、社会危害大的侵权盗版分子一律依法从严查处。欢迎广大网民积极投诉举报，提供侵权盗版案件线索。各级版权相关执法部门将推动网络企业积极履行主体责任，共同构建打击网络侵权盗版社会共治格局。（来源：北京商报）

- **国家版权局等关于开展打击网络侵权盗版“剑网 2020”专项行动的通知**
- **全文：**http://www.ncac.gov.cn/chinacopyright/contents/483/417532.html

➢ 市场监管总局等六部门印发《国家电子政务标准体系建设指南》

2020 年 6 月 18 日，国家市场监督管理总局、中共中央办公厅机要局、国务院办公厅电子政务办公室、中央网信办秘书局、国家发展改革委办公厅、工业和信息化部办公厅六部门关于印发《国家电子政务标准体系建设指南》的通知。

各省、自治区、直辖市及新疆生产建设兵团市场监管局（厅、委）、机要局、政府办公

厅、网信办、发展改革委、工业和信息化主管部门，有关标准化技术委员会：

为加强电子政务领域标准化顶层设计，推动电子政务标准体系建设，支撑电子政务实施应用，现将《国家电子政务标准体系建设指南》印发给你们，请认真贯彻执行。（来源：国家市场监督管理总局）

- **关于印发《国家电子政务标准体系建设指南》的通知**
- **全文：**http://gkml.samr.gov.cn/nsjg/bzjss/202006/t20200618_317126.html

➢ 自然资源部印发《2020 年自然资源部网络安全与信息化工作要点》

2020 年 6 月 2 日，自然资源部印发《2020 年自然资源部网络安全与信息化工作要点》，要求推进自然资源三维立体“一张图”和国土空间基础信息平台建设，在统一的国土空间基础信息平台上，加强三维立体可视化与分析应用功能建设，初步形成统一、高效、互联互通的自然资源管理、应用和共享服务机制。

为认真落实《自然资源部信息化建设总体方案》和 2020 年全国自然资源工作会议确定的重点任务，推动新一代信息技术与自然资源管理的深度融合，提升自然资源治理能力和水平，6 月 9 日，自然资源部印发《2020 年自然资源部网络安全与信息化工作要点》（以下简称《工作要点》），部署推进自然资源三维立体“一张图”和国土空间基础信息平台建设、深化自然资源政务管理系统集成与应用、促进自然资源数据共享与服务、促进自然资源调查监测数字化、加强自然资源网络与信息化安全、强化自然资源信息化统筹等重点工作。

《工作要点》提出，充分利用基础测绘成果，以数字高程模型（DEM）等三维测绘成果为基底，以遥感影像为背景，集成整合地下空间、地表基质、地表覆盖、业务管理等各类自然资源和国土空间数据，按照统一的标准，构建自然资源三维立体“一张图”，全面真实地反映自然资源现实状况和自然地理格局，为核实、检验各类调查成果和上报数据的真实性提供基础，为国土空间规划、用途管制、耕地保护、督察执法、审批监管等自然资源管理和决策提供重要支撑和保障。

《工作要点》要求通过国土空间基础信息平台，实现自然资源管理与服务的精准化和高效化。完善国土空间基础信息平台的分布式应用和服务架构，建立统一身份认证、统一用户管理、统一电子签章、统一电子证照、统一安全审计等基础服务。在统一的国土空间基础信息平台上，加强三维立体可视化与分析应用功能建设，初步形成统一、高效、互联互通的自

然资源管理、应用和共享服务机制。

另外，《工作要点》要求加强自然资源信息化的统一领导和管理，重点开展自然资源信息化战略研究，整体谋划“十四五”自然资源信息化工作，研究编制自然资源业务信息化应用系统建设指南，编制省及省以下自然资源信息化“十四五”规划或总体方案。（来源：中华人民共和国自然资源部）

- **自然资源部办公厅关于印发《2020 年自然资源部网络安全与信息化工作要点》的通知**
- **全文：**http://gi.mnr.gov.cn/202006/t20200609_2525658.html

➢ 工业和信息化部发布关于加强呼叫中心业务管理的通知

2020 年 6 月 18 日，工业和信息化部印发《关于加强呼叫中心业务管理的通知》（工信部信管〔2020〕81 号，以下简称《通知》），现就有关内容解读如下：

一、《通知》出台的背景是什么？

严控骚扰电话，保障人民群众合法权益是践行以人民为中心的发展思想的重要举措，工业和信息化部高度重视，2018 年以来，联合教育部、住建部、银保监会等 12 个部门开展综合整治骚扰电话专项行动，取得一定成效。但期间，利用 95/96 号码拨打骚扰电话问题突出，老百姓反映强烈，给治理工作带来负面影响。分析原因，其中一部分是由于呼叫中心企业守法意识淡薄，重利益轻责任，管理措施不到位，为商业营销企业拨打骚扰电话提供便利。

为引导和规范呼叫中心企业良性发展，回归服务用户信息咨询的业务形态，杜绝相关骚扰电话扰民问题，工业和信息化部拟加大整治力度，从严规范呼叫中心企业经营行为，在深入调研、广泛征求意见的基础上，出台《通知》。对于其他商业营销企业拨打骚扰电话的问题，工业和信息化部将继续会同相关部门，加强源头治理，合力斩断骚扰电话利益链。

二、加强呼叫中心业务管理的思路是什么？

总体思路是：坚持问题导向，抓住市场准入、码号管理、接入管理、经营行为管理和违规处置等五个关键环节，从严规范，力争短时间内有效遏制呼叫中心企业利用 95/96 号码拨打骚扰电话问题。

具体而言，一是规范呼叫中心经营行为，强化主体责任落实，引导回归用户信息咨询业务形态，要求合法合规使用电信资源、保障用户信息安全、严禁拨打骚扰电话。二是强化基础电信企业接入管理责任，明确不得提供接入的情形，斩断骚扰电话通信渠道。三是加强监

督检查和执法，电信管理机构从严准入管理、码号管理，依法处理违规行为，强化监督管理。

三、《通知》包括哪些主要内容？

《通知》共包括六个部分，针对呼叫中心业务管理相关环节，明确管理要求：

一是加强准入管理。重申呼叫中心业务形态，明确要求不允许提供商业营销类电话呼出服务。要求电信管理机构对申请企业进行实地查验，不符合条件的不予受理许可申请或者不予许可。同时，明确在用户同意情况下的可以呼出的情况。

二是加强码号管理。要求原则上呼叫中心电信业务接入号码只开通呼入功能。呼叫中心业务经营者在开通业务前，须按规定如实备案电信业务接入号码接入的基础电信企业、使用用途、呼入呼出开通情况等，不得擅自转让、出租等违规使用码号资源。

三是加强接入管理。要求基础电信企业提供接入服务前，核实必要信息并留存记录，对不符合要求的不得提供接入服务。在合同协议中明确具体要求，严格按照相关要求提供接入服务。建立完善相关管理机制和技术手段，从事前、事中、事后分别采取相应措施加强资源管理，防范违规使用，审慎与存在骚扰电话问题的企业合作。

四是加强经营行为管理。要求呼叫中心企业健全内部管控机制，建立技术手段，严格控制呼出，禁止拨打骚扰电话或为拨打骚扰电话提供便利，留存不少于 30 日的通话记录等信息，不得擅自转租转售语音中继线路等通信资源，不得违规更改、隐藏电信业务接入号码，并保障用户个人信息安全。

五是明确相关事项。明确仅提供呼叫中心系统和坐席出租服务的也属经营呼叫中心业务，要求相关经营者核实用户语音中继和号码的合法性和防范骚扰电话。明确自用类型、人力外包、技术服务等不属于经营呼叫中心业务的情况。同时，根据我部《开展第二类增值电信业

务相关许可事项告知承诺审批试点工作实施方案》（工信厅信管〔2019〕86 号），自由贸易试验区内申请经营呼叫中心业务符合告知承诺试点条件的，按照相关要求执行。

六是明确相关工作要求。要求相关企业提高思想认识，坚决落实《通知》要求，遏制拨打骚扰电话扰民。要求相关企业立即开展自查，自觉纠正不符合《通知》要求的行为，并于2020年7月底前完成自查整改。要求将呼叫中心企业因骚扰电话问题被有关政府部门通报、约谈、行政处罚等依法纳入电信业务经营不良和失信名单，电信管理机构、基础电信业务经营者分别在新增许可、接入号码备案及新增接入、合作等环节进行信用约束。

四、在《通知》后续实施方面有哪些考虑？

《通知》下发后，工业和信息化部将从宣贯、执行、监督检查等方面着手，保障《通知》工作要求落到实处。

一是加强政策宣贯。做好对企业的政策咨询和引导工作，引导呼叫中心企业合法合规经营业务，营造良好市场环境。

二是抓好执行落实。根据《通知》要求，组织各地通信管理局、基础电信企业、呼叫中心企业等落实准入管理、码号管理、接入管理、合法经营等事项，督促相关企业自查自纠，抓好呼叫中心业务规范管理，推动解决呼叫中心企业利用 95/96 号码拨打骚扰电话问题。

三是加强监督检查。组织各通信管理局利用双随机检查等机制，强化对呼叫中心业务合法合规经营情况的检查。对存在违规行为的，视情节严重程度，依法通过约谈、曝光、行政处罚等方式，进行追责问责。落实企业主体责任，督促企业自觉守法合规经营。（来源：工业和信息化部信息通信管理局）

- **工业和信息化部关于加强呼叫中心业务管理的通知工信部信管〔2020〕81 号全文：**
- http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c7979380/content.html

五、本期重要漏洞实例

➢ Cisco IOS XE 命令注入漏洞

发布日期：2020-06-9
更新日期：2020-06-9
受影响系统：
Cisco Catalyst 3650 Series Switches
Cisco Catalyst 3850 Series Switches
Cisco Catalyst 9300 Series Switches
Cisco Catalyst 9200 Series Switches
Cisco Catalyst 9500 Series Switches
描述：

CVE(CAN) ID: CVE-2020-3207
Cisco IOS XE 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 XE Software 中引导程序选项的处理存在命令注入漏洞，该漏洞源于处理引导程序选项时未充分验证输入信息。攻击者可通过修改设备引导程序选项利用该漏洞绕过安全启动过程，并以 root 权限在受影响的设备上执行恶意代码。
建议：

厂商补丁：
Cisco
目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ngwc-cmdinj-KEwWVWR

➢ Microsoft 发布 2020 年 6 月安全更新

发布日期：2020-06-9
更新日期：2020-06-9
描述：
6 月 9 日，微软发布了 2020 年 6 月份的月度例行安全公告，修复了其多款产品存在的 128 个安全漏洞。受影响的产品包括：Windows 10 2004 & WindowsServer v2004（89 个）、Windows 10 1909 & WindowsServer v1909（88 个）、Windows 10 1903 & WindowsServer v1903（90 个）、Windows 8.1 & Server 2012 R2（36 个）、Windows RT 8.1（36 个）、Windows Server 2012（35 个）、Microsoft Edge (EdgeHTML-based)（4 个）、Internet Explorer（8 个）和 Microsoft SharePoint-relatedsoftware（15 个）利用上述漏洞，攻击者可以绕过安全功能限制，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-2020-1301	**Windows SMB 远程代码执行漏洞** Microsoft Server Message Block 1.0 (SMBv1)服务器处理某些请求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目标服务器上执行代码。要利用此漏洞，在大多数情况下，经过身份验证的攻击者可以向目标 SMBv1 服务器发送精心编制的数据包。 安全更新通过更正 SMBv1 如何处理这些精心编制的请求来解决该漏洞。	重要 远程执行代码	Windows 10 Server 2016 Server 2019 Server, version 1803 Server, version 1903 Server, version 1909 Server, version 2004 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-1286	**Windows Shell 远程代码执行漏洞** 当 Windows Shell 未能正确验证文件路径时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在当前用户的上下文中运行任意代码。如果当前用户以管理员身份登录，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；或者使用提升的权限创建新帐户。将帐户配置为在系统上具有较少权限的用户可能比使用管理权限操作的用户受影响较小。 此安全更新通过确保 Windows Shell 正确验证文件路径来解决此漏洞。	严重 远程执行代码	Windows 10 Server 2019 Server, version 1803 Server, version 1909 Server, version 1903 Server, version 2004
CVE-2020-1292	**OpenSSH for Windows 权限提升漏洞** 当 OpenSSH for Windows 未正确限制对配置设置的访问时，存在权限提升漏洞。成功利用此漏洞的攻击者可以用恶意二进制文件替换外壳。要利用此漏洞进行攻击，经过身份验证的攻击者需要在易受攻击的系统上修改 OpenSSH for Windows 配置。然后，攻击者需要说服用户连接到易受攻击的 OpenSSH for Windows 服务器。 此更新通过限制对 OpenSSH for Windows 配置设置的访问来解决此漏洞。	重要 特权提升	Windows 10 Server 2019 Server, version 1803 Server, version 1909 Server, version 1903 Server, version 2004
CVE-2020-1248	**GDI+远程代码执行漏洞** Windows Graphics Device Interface (GDI)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。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 Windows GDI 处理内存中对象的方式来解决该漏洞。	严重 远程执行代码	Windows 10 Server, version 1903 Server, version 1909 Server, version 2004

CVE-2020-1239	**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。攻击者可以通过多种方式利用此漏洞，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。	重要 远程执行代码	Windows 10 Server 2016 Server 2019 Server, version 1803 Server, version 1903 Server, version 1909 Server, version 2004 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-1300	**Windows 远程代码执行漏洞** 当 Microsoft Windows 未能正确处理压缩文件时，存在远程代码执行漏洞。要利用此漏洞，攻击者必须说服用户打开精心编制的 cabinet 文件或欺骗网络打印机，并诱使用户安装伪装为打印机驱动程序的恶意 cabinet 文件。 此更新通过更正 Windows 如何处理压缩文件来解决此漏洞。	重要 远程执行代码	Windows 10 Server 2016 Server 2019 Server, version 1803 Server, version 1903 Server, version 1909 Server, version 2004 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-1281	**Windows OLE 远程代码执行漏洞** 当 Microsoft Windows OLE 未能正确验证用户输入时，存在远程代码执行漏洞。攻击者可以利用此漏洞执行恶意代码。要利用此漏洞，攻击者必须说服用户从网页或电子邮件中打开精心编制的文件或程序。更新通过更正 Windows OLE 如何验证用户输入来解决此漏洞。	严重 远程执行代码	Windows 10 Server 2016 Server 2019 Server, version 1803 Server, version 1909 Server, version 1903 Server, version 2004 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-1073	**Scripting Enginel 内存破坏漏洞** ChakraCore 脚本引擎处理内存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。 安全更新通过修改 ChakraCore 脚本引擎如何处理内存中的对象来解决该漏洞。	严重 远程执行代码	Microsoft Edge(EdgeHTML-based) ChakraCore

CVE-2020-1260	**VBScript 远程代码执行漏洞** VBScript 引擎处理内存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。 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 9 Internet Explorer 11
CVE-2020-1181	**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.Netweb 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。 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。	严重 远程执行代码	SharePoint Enterprise Server 2016 SharePoint Server 2019 SharePoint Foundation 2010 SharePoint Foundation 2013

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

➢ IBM WebSphere Application Server 代码问题漏洞

发布日期：2020-06-12
更新日期：2020-06-12
受影响系统：
IBM WebSphere Application Server 8.5
IBM WebSphere Application Server 9.0
描述：

CVE(CAN) ID: CVE-2020-4450
IBM WebSphere Application Server（WAS）是美国 IBM 公司的一款应用服务器产品。该产品是 JavaEE 和 Web 服务应用程序的平台，也是 IBMWebSphere 软件平台的基础。
IBM WebSphere Application Server 存在代码问题漏洞。攻击者可利用该漏洞执行任意代码。
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/security-bulletin-websphere-application-server-vulnerable-remote-code-execution-vulnerability-cve-2020-4450

➢ Apple macOS Catalina Wi-Fi 组件内存破坏漏洞

发布日期：2020-06-10
更新日期：2020-06-10
受影响系统：
Apple macOS Catalina <10.15.5
描述：

CVE(CAN) ID: CVE-2020-9834
Apple macOS Catalina 是美国苹果（Apple）公司的一套专为 Mac 计算机所开发的专用操作系统。Wi-Fi 是其中的一个无线上网组件。
Apple macOS Catalina 10.15.5 之前版本中的 Wi-Fi 组件存在内存破坏漏洞，攻击者可利用该漏洞以内核权限执行任意代码。
建议：

厂商补丁：
Apple
厂商已发布了漏洞修复程序，请及时关注更新：
https://support.apple.com/zh-cn/HT211170

六、本期网络安全事件

➢ 本田汽车全球业务网络被勒索软件攻击 部分产线被迫停工

2020 年 6 月 11 日，如果公司遭到了勒索病毒的攻击，由于该病毒独特的加密机制，被攻击方除了缴纳赎金之外，往往没有更好的解决办法。而当下，本田汽车就遇到了这件麻烦事。

日前，本田汽车在推特上发布声明称，公司内部的全球业务网络可能遭到了网络攻击，致使一些工厂产线被迫停产，部分全球业务无法办理。此前，该公司还发布了一条推文，声明其客户服务和金融服务因黑客攻击“不可用”。

本田在向 The Verge 发表的一份声明中说道：“目前没有证据表明个人身份信息丢失。我

们大多数工厂都已恢复生产，目前正在努力恢复我们在俄亥俄州的汽车和发动机工厂的生产工作。”同时，该公司表示，受影响的工厂预计最早将于近两天恢复运营。

据本田工作人员透露，其遭受的网络攻击所使用的攻击软件，可能是 Snake 的勒索软件。该软件可将内部网络上的文件加密，只有在支付赎金后才会被解密。据悉，Snake 是一种新的勒索软件，往往针对企业来进行攻击，使用 Golang 编写，被加密文件末尾在追加 EKANS，反过来就是 SNAKE。最重要的是，该病毒不支持解密，意味着被攻击者只能缴纳赎金，才能恢复文件。（来源：新浪科技）

➢ 郑州某高校两万名学生信息遭泄露，副校长等被行政处罚

2020 年 6 月 10 日报道，针对媒体报道的郑州西亚斯学院学生信息遭泄露一事，继涉事学校 10 日公开发布致歉声明后，当日晚间，郑州警方发布消息称，警方依据《中华人民共和国网络安全法》，对郑州西亚斯学院、及负有领导责任的一名副校长和直接责任人进行了行政处罚。

据有关报道，郑州西亚斯学院多名学生反映称，学校近两万学生个人信息被泄露，以表

格的形式在微信、QQ 等社交平台上流传。

针对此事件，郑州西亚斯学院 10 日通过官网发布致歉声明称，近日，该校在返校复学准备工作中发生了部分学生个人信息泄露事件，由此给学生和家长带来的不便，表示深深的歉意，向社会各界人士、广大网友、媒体的关心和批评表示诚恳的感谢。

声明称，该校在积极准备学生返校复学时，按照疫情防控要求，由教务科研处整理了计划返校学生名单，用以核查学生返校来源地及个人健康状况等信息。由于工作人员缺乏保密意识，造成部分学生的个人信息泄露，学校负有不可推卸的责任。事件发生以来，学校在公安机关的帮助下查清了事情原委，及时成立三个工作专班，明确分工，专项排查，第一时间通知师生保护信息安全，不得随意转发，有效地控制了信息的进一步扩散。

同时，学校对直接责任人予以解除劳动合同，对相关部门负责人及两名主管校领导予以记过处分，并将配合公安机关对其他涉嫌违法的行为严肃追究。

声明表示，通过这次事件，意识到管理工作存在严重缺陷和不足，学校将尽最大努力弥补事件造成的损害，要求有关部门在全校范围内开展信息安全隐患排查。在今后的工作中，将深刻吸取教训，更加注重细节，坚决封堵漏洞，努力做到学生满意、家长放心、社会认可。

公开资料显示，郑州西亚斯学院地处郑州新郑市，学校始建于 1998 年，前身是由郑州工业大学参与举办的中外合作办学机构郑州工业大学西亚斯国际工商管理学院。2000 年，原郑州工业大学并入郑州大学，学院更名为郑州大学西亚斯国际学院。2018 年，学院脱离郑州大学独立办学，更名为郑州西亚斯学院。

当日晚间，来自郑州警方的消息称，目前，新郑市公安局依据《中华人民共和国网络安全法》对郑州西亚斯学院、及负有领导责任的一名副校长和直接责任人进行了行政处罚。（来源：中新网）

➢ POS 植入病毒韩国 90 万张信用卡个人信息遭泄露！

2020 年 6 月 9 日，韩国《每日经济》报道，韩国信贷金融协会 8 日表示，据金融保安院调查，韩国约有 90 万张信用卡信息正在外国网络黑市上非法流通，其中，除有效期到期，补发等情况外，实际可使用的有效信用卡约有 41 万张。

据确认的加盟店分析结果显示，此次泄露的信用卡信息是韩国引进 IC 终端机之前通过感染了恶性代码的 POS 终端等被黑客窃取的（手机 POS 机是一种 RF-SIM 卡终端阅读器）。信贷协会方面正在掌握信用卡信息被盗的途径，计划与金融保安院合作对相关加盟店采取保安措施等。此外，协会还计划推进相关信用卡公司对不正当使用事故全额赔偿的方案，最大限度地减少对信用卡持卡人的直接损失。

据悉，本次信用卡个人信息大规模泄漏已不是第一次。早在 2014 年，韩国就曾发生超大规模的个人信息泄露事件，事件中，个人信用评估公司职员非法收集并泄露信用卡客户个人信息高达 1 亿 400 万条，涉及 KB 国民卡、乐天卡及 NH 农协卡三家公司，为迄今为止韩国史上规模最大的信用卡个人信息泄漏事件。（来源：韩国《每日经济》报道）

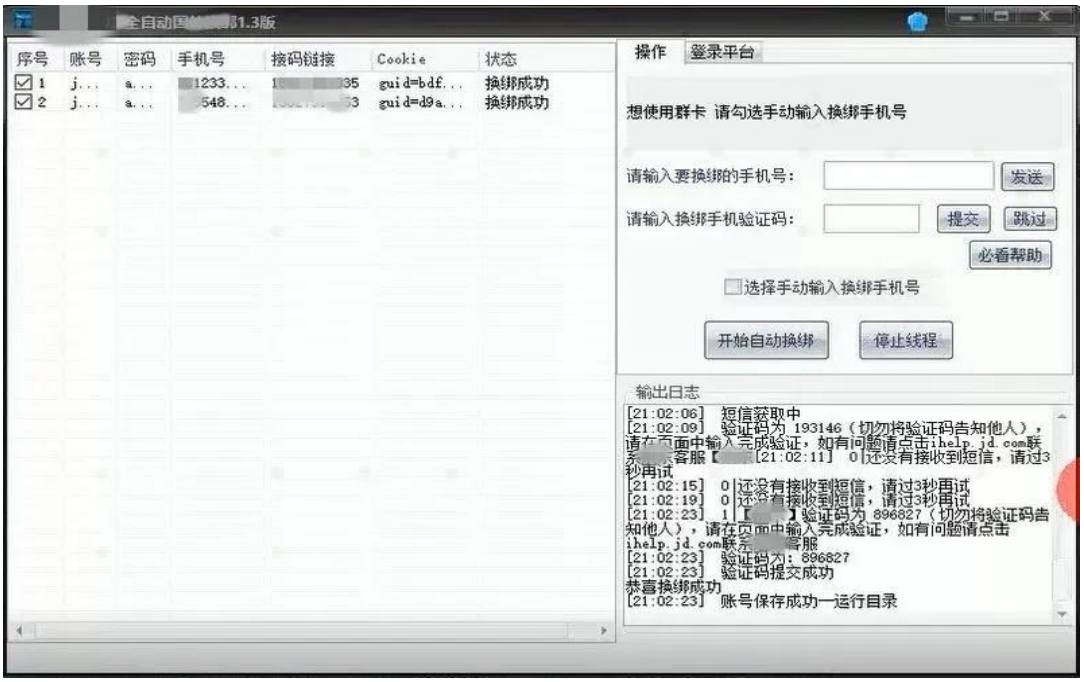
➢ 男子非法制售软件“薅羊毛”致电商损失 400 余万元被刑拘

2020 年 6 月 15 日报道，近日，北京大兴警方在“净网 2020”专项行动中，深挖线索，查获一名藏身网络的幕后黑手，破获一起非法制作并出售“薅羊毛”软件案。嫌疑人王某某制作的非法软件能够绕过平台风控系统，侵入电商网络系统专门领取优惠券、现金红包，造成某电商企业损失 400 余万元，王某某出售软件获利 20 余万元。

今年 4 月，某电商平台报警，称有人利用非法软件绕过平台风控系统，疯狂骗取优惠券、现金红包，造成企业损失 400 余万元。对此，在市公安局网安总队的指导下，大兴公安分局组织专业警力开展调查工作，通过调取后台数据，发现至少有 3 款非法软件异常进入电商网

络系统专门领取优惠券。为查明真相，找出幕后黑手，警方通过对相关非法软件进行细致研究，层层破译，终于锁定了嫌疑人王某某(男，24 岁，山东省人)，并在昌平区一出租房内将其抓获。

据王某某交代，其对软件制作非常感兴趣，曾经加入过一些技术开发类的 QQ 群，从中认识了几名“志同道合”的网友。在看到有人开发非法软件获利后，他也尝试购买了一条软件源代码，并发挥“聪明才智”与专业特长，改写制作出能够进入电商平台系统调用端口数据篡改设备信息的软件，且通过 QQ 群进行售卖。



尝到甜头后，他又根据不同“市场需求”，陆续研发出多款软件，累计获利 20 余万元。特别是疫情期间，他更是在家专心做起了“产品研发”“产品升级”“售后服务”等工作。目前，王某某因涉嫌违反《刑法》第二百八十五条第三款相关罪名已被大兴警方刑事拘留。

北京警方提示：君子爱财，取之有道。即便是在虚拟的网络世界，也要做到诚信购物，使用非法软件骗取商家优惠，既破坏了公平的市场秩序，也为不法分子提供了生存的土壤。网络社会不是法外之地，一切违法犯罪都终将受到法律的制裁。（来源：北京日报）

➢ 福州一男子在多家酒店装摄像头:600 多人被偷拍 获刑 7 个月

2020 年 6 月 11 日，福建省福州市鼓楼区人民法院审结了一起非法使用窃听、窃照专用器材案，被告人陈某在短短两个月内，在多家酒店安装针孔摄像头，偷拍酒店房间入住人员达到 600 余人次，其中下载性爱视频 42 段、隐私照片 109 张。法院以非法使用窃听、窃照专用器材罪判处陈某有期徒刑七个月。事实上，如此偷拍事件并不罕见，记者此前调查发现，摄像头偷拍的背后，有一条非法安装、上传、共享、买卖交易的黑色产业链。

针孔摄像头藏于酒店房间空调管道上两月内偷拍房客 600 余人次

根据鼓楼区人民法院披露的案件细节，2019 年 4 月，陈某到福州就职，同年 5 月，陈某在浏览网页时无意间看到有卖针孔摄像设备的信息，在不良思想作祟下，动了偷窥别人私密生活的念头，于是在短短两个月内陆续从该网络交易平台上以每套设备一百余元的价格陆续购买了 4 套设备，包含储蓄卡、针孔摄像头、电源设置以及下载在手机终端的 APP，并附

带具体安装操作和使用说明书。

2019 年 7 月，陈某以居住酒店的名义进入酒店房间，按照网页教程把摄像设备安装在房间内的空调管道上，调整摄像头对着房间床铺的位置便于拍摄。而后，他以相同的手段在多家酒店安装摄像设备。而后，每当房间有人入住，陈某便时时打开 APP 在线观看，而性爱视频是其观看录制和存储的重点。

2019 年 11 月，公安民警根据举报的线索将陈某抓获，当场从其身上查获安装监控视频、存储着偷拍视频和照片的手机及储存卡等物品。之后，在公安民警监督带领下，陈某将酒店内安装的非法设备一一拆除。经查，作案期间，陈某共对 600 余人进行偷拍，其中下载性爱视频 42 段、隐私照片 109 张。

根据《刑法》第二百八十四条规定，非法使用窃听、窃照专用器材，造成严重后果的，处二年以下有期徒刑、拘役或者管制。最终，法院以非法使用窃听、窃照专用器材罪判处陈某有期徒刑七个月。同时，认为陈某的行为侵害众多不特定公民的隐私权，应承担民事侵权责任，责令陈某删除本案中所有涉及侵犯他人隐私的照片及视频，以消除影响，并在国家级媒体上向社会公众公开赔礼道歉。（来源：界面新闻）

➢ 河北一街道办工作人员泄露疫情隐私被拘

2020 年 6 月 17 日，自新发地菜市场爆发新冠疫情以来，北京的防控措施不断升级。临近北京的河北燕郊一街道办工作人员贾某某，因在微信群传播《紧急突发事件快速报告表》涉嫌侵犯公民个人隐私被依法拘留 10 日。新冠肺炎暴发以来，记者注意到，各地频频发生疫情相关个人隐私泄露事件。

燕郊一街道工作人员因泄露疫情信息被拘留

自北京疫情爆发以来，北京及周边地区都在寻找去过新发地市场的居民。几日前，燕郊居民的微信群里面流传着“福成二期有居民去过新发地市场，全家低烧并报警”的信息。据河北三河市网信办消息，6 月 14 日 8 时许，河北省三河市公安局也注意到了这一情况，流传的信息中涉及到居民张某等人的隐私信息。

15 日上午，经民警多方工作查明，13 日 20 时 2 分许，燕郊高新区一街道办工作人员贾某某（男，28 岁）在街道办的值班微信群内看到《紧急突发事件快速报告表》文件，立即将该文件的传真件照片转发至其所在的家庭群内（群成员 7 人），随后该文件扩散至外部

社会微信群内，并在三河本地微信群造成大量传播。此外，三河市疾控中心 14 日回应，被泄露隐私的张某一家三口核酸检测均为阴性。目前，违法嫌疑人贾某某因侵犯公民个人隐私已被三河市公安局依法行政拘留 10 日，并处罚款 500 元。6 月 17 日，河北三河市网信办官方微信公众号通报。

延展：各地频发疫情相关个人隐私泄露事件

疫情暴发以来，各地频频发生疫情相关个人隐私泄露事件。春节前后，针对返乡人员的信息登记在全国各地开展，包含身份证号等信息的名单在各种微信群肆意流传。记者调查发现，有近 7000 多名武汉返乡人员的信息被泄露。当时有知情者透露，信息泄露源头和登记返乡人员的途径直接相关。

3 月中旬，国内疫情形势趋缓，境外输入病例开始受关注。郑州首例输入病例郭某鹏因隐瞒出境史、未严格落实隔离观察引发民众不满，随后其身份证号、手机号等信息被曝光。

4 月中旬，在疫情防控常态化条件下，青岛胶州中心医院因出现多名新冠肺炎确诊病例和无症状感染者而受到关注。在当地发布寻找近期过去该院的紧急寻人启事后，一份包含 6000 余人电话、门牌号、身份证号、就诊类型的详细名单在当地流传。

4 月初，黑龙江省哈尔滨市、牡丹江市相继发生境外新冠肺炎输入病例关联的本土聚集性疫情。4 月 20 日，黑龙江省牡丹江市纪委监委发布公职人员疫情防控期间有关纪律规定，其中特别要求 “不得通过互联网、社交软件等途径捏造、传播、散布谣言，要保守工作秘密，不擅自发布、传播、泄露非公开发布的疫情防控工作信息。4 月中旬，胶州中心医院就诊人员名单泄露后，当地警方迅速展开调查，对最初泄露信息的 3 名工作人员给予

行政拘留处罚。（来源：南方日报）

信息安全意识产品服务

021-33663299