国盟信息安全通报

2020 年 1 月 06 日第 209 期

全国售后服务中心

国盟信息安全通报

（第 209 期）

国际信息安全学习联盟

2020 年 01 月 06 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 203 个，其中高危漏洞 67 个、中危漏洞 118 个、低危漏洞 18 个。漏洞平均分值为 5.83。本周收录的漏洞中，涉及 0day 漏洞 93 个（占 46%），其中互联网上出现“libIEC61850 'BerDecoder_decodeUint32'函数缓冲区溢出漏洞、RIOT RIOT-OS 拒绝服务漏洞”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 3493 个，与上周（3156 个）环比增长 10%。

主要内容

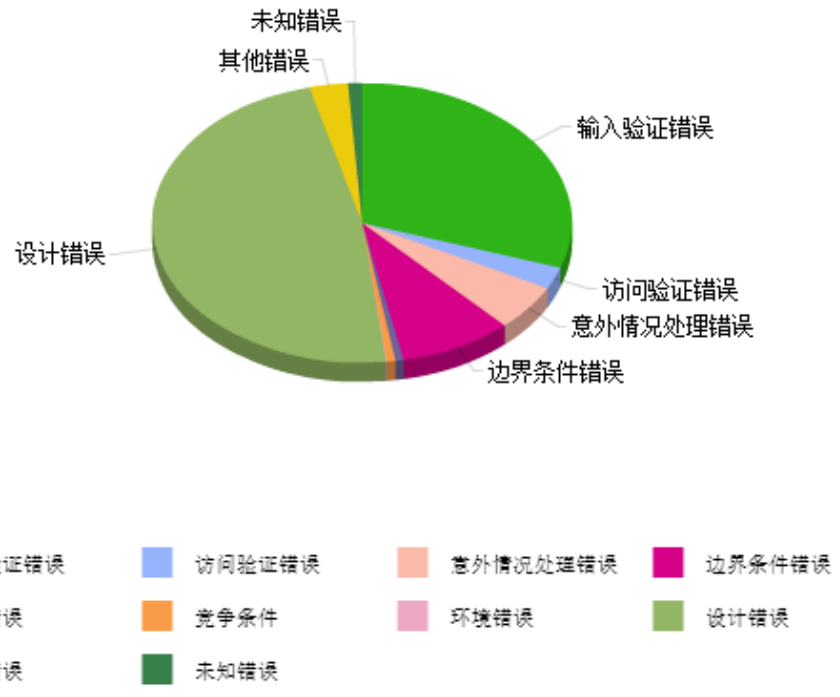
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

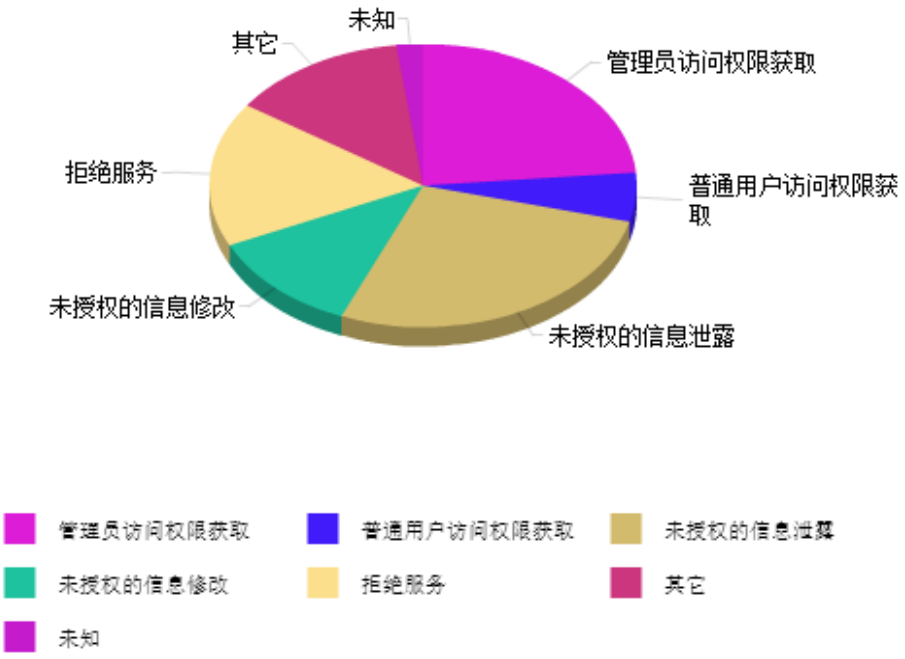
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 203 个，其中高危漏洞 67 个、中危漏洞 118 个、低危漏洞 18 个。漏洞平均分值为 5.83。本周收录的漏洞中，涉及 0day 漏洞 93 个（占 46%），其中互联网上出现“libIEC61850 'BerDecoder_decodeUint32'函数缓冲区溢出漏洞、RIOT RIOT-OS 拒绝服务漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3493 个，与上周（3156 个）环比增长 10%。

二、安全漏洞增长数量及种类分布情况

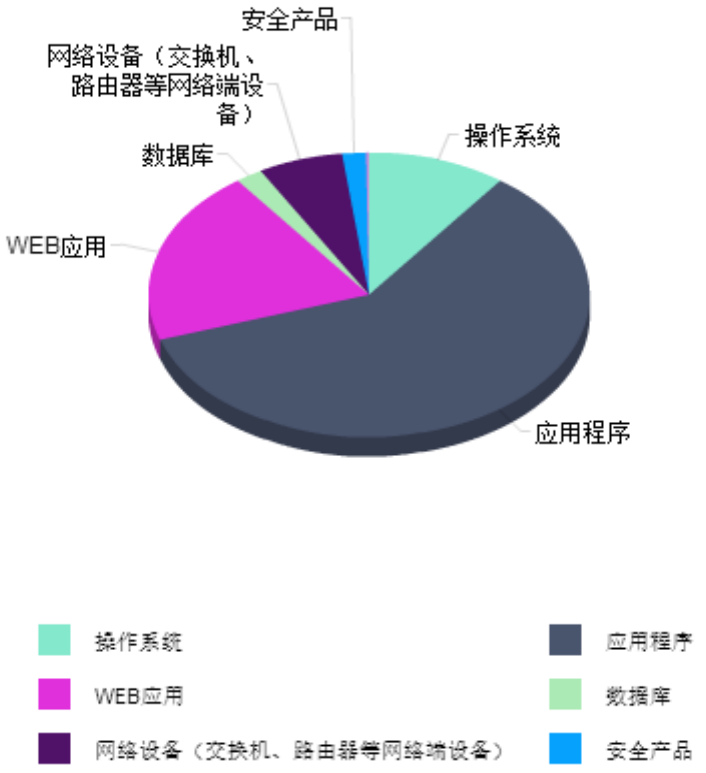
➢ 漏洞产生原因（2019 年 12 月 23 日—2020 年 01 月 06）



➢ 漏洞引发的威胁（2019 年 12 月 23 日—2020 年 01 月 06）



➢ 漏洞影响对象类型（2019 年 12 月 23 日—2020 年 01 月 06）



三、安全产业动态

➢ 《密码法》，究竟跟你我生活有多大关系？

2019 年 10 月 26 日，十三届全国人大常委会第十四次会议审议通过《中华人民共和国密码法》，习近平主席签署 35 号主席令予以公布，自 2020 年 1 月 1 日起正式施行。密码法是国家安全法律体系的重要组成部分，是我国密码领域的首部综合性、基础性法律。那么，密码法中所说的密码是指什么？密码与国家安全、经济社会发展，以及我们的日常生活有着什么样的关系呢？

提起密码很多人并不陌生，人们通常以为就是每天接触的计算机或手机开机“密码”、电子邮箱登录“密码”、银行卡支付“密码”等。生活中的这些“密码”实际上是口令。口令只是进入计算机、手机、电子邮箱或个人银行账户的“通行证”，它是一种简单、初级的身份认证手段，是最简易的密码。密码法中说的密码指的是什么呢？

国家密码管理局新闻发言人李国海说：“密码法中的密码就是采用特定变换对信息等进行加密保护和安全认证的技术、产品和服务。密码的功能主要有两个，一个是加密保护，一个是安全认证。密码的这两大特殊功能，决定了密码在网络空间中身份识别、安全隔离、完整性保护、信息加密和抗抵赖性等方面，具有不可替代的重要作用。”

简单地说，加密保护就是把明文变成密文，将原来可读的信息变成不能识别的符号序列。我们日常生活中常用的移动支付、扫码乘车等等都需要密码技术来保障安全。再比如，家家户户用的智能电表也应用了密码技术。

我们现在下载手机 APP 就可以交电费，或者使用充值卡缴费，方便快捷的背后都源于密码技术的安全保护。除了移动支付，大家熟悉的二代身份证、电子发票等都采用了密码技

术，在保护公民身份信息、维护经济安全方面发挥了重要作用。正是由于密码技术的迅猛发展和广泛应用，催生了密码法的诞生。密码法是一部什么样的法律，它都有哪些内容呢？

李国海说：“密码法系统总结长期以来密码工作经验，以法律的形式确立了我国密码工作的领导和管理体制及根本原则，明确对核心密码、普通密码、商用密码实行分类管理。”

国家对密码实行分类管理，密码分为核心密码、普通密码和商用密码三类。核心密码、普通密码用于保护国家秘密信息。核心密码保护信息的最高密级为绝密级。普通密码保护信息的最高密级为机密级。商用密码用于保护不属于国家秘密的信息。

密码法一共五章四十四条，内容围绕怎么用密码，谁来管密码，怎么管密码展开。制定密码法就是要规范全社会密码应用，通过对密码实施分类管理，引导社会正确、合规、有效使用密码，真正发挥密码在维护国家安全中的重要作用。

在人类的历史长河中，密码始终给人一种神秘的印象。在相当长的时期内，密码与政治和军事斗争密不可分，无论是在古代战场，还是在现代战争中，密码都扮演着重要的角色，是交战双方加密、破译、传递机密、获取情报的重要手段，也因此成为许多影视剧特别是谍战剧中的重要元素。现如今密码被广泛应用于政治、经济、社会各个方面，在网络时代，密码是维护网络空间安全的重要法宝，是构筑网络信息系统免疫体系和网络信任体系的基石，直接关系国家政治安全、经济安全、国防安全和信息安全，是保护党和国家根本利益的战略性资源，是实现国家治理体系和治理能力现代化的重要支撑。

密码的发展离不开科技的支撑，密码的较量说到底是技术和人才的较量。今年已经 85 岁高龄的中国工程院院士蔡吉人，从事密码科研工作已经 60 多年，见证了我国密码从弱到强、从小到大的发展历程。

蔡吉人说：“密码应用已不局限于党政军领导机关和机密要害部门，已经遍及社会、经济生活的各领域。我体会到密码最大的特点，是它的核心技术，它是买不来、要不到的。买来了、要来了也不敢用，就是靠自力更生、自主创新。”

随着科技的进步，密码学研究在我国快速发展。我国自主设计了首个数字签名标准算法：SM3 密码算法，已经成为我国电子认证、网络安全通信、云计算与大数据安全等领域的基础性密码算法。

党的十八大以来，我国密码事业进入了发展的快车道，密码科技创新和产业支撑能力显著增强，形成了从密码芯片到密码服务的完整产业链条，密码应用广度和深度大幅提升，在金融、教育、税务、交通、工业制造等重要领域得到广泛应用。例如增值税防伪税控系统使用商用密码技术，实现网上缴税电子税票等方面的应用，有效遏制了偷税、漏税、税票造假

等违法行为，每年为国家防范税收流失 1000 亿元以上。

2014 年 4 月，习近平总书记首次提出总体国家安全观。近年来，国家安全法、反间谍法、反恐怖主义法、网络安全法、国家情报法等法律相继出台，国家安全立法全面推进，改变了过去主要依靠规章和规范性文件管理的局面，网络安全立法的四梁八柱已经初步搭建。密码法是国家安全法律体系的重要组成部分。

密码法中明确规定，坚持中国共产党对密码工作的领导，中央密码工作领导机构对全国密码工作实行统一领导，这是由密码工作性质、地位和历史决定的。党的密码工作创建于烽火硝烟的 1930 年，是毛泽东、周恩来等老一辈无产阶级革命家创建的，一代代密码工作者紧紧追随党中央、服务党中央，全力确保了党中央指示政令军令安全畅通。周恩来同志是我们党的密码工作的开创者，他亲自创编了我党第一本密码“豪密”，率先提出了改革密码的思想。直到生命的最后时刻，还审阅了重要的密码编制报告，为我党密码工作建设和发展呕心沥血、鞠躬尽瘁。90 年来，密码工作在党领导革命、建设和改革的各个时期发挥了不可替代的重要作用，进入新时代，密码工作仍面临着许多新的机遇和挑战。

国家密码管理局局长李兆宗说：“制定和实施密码法，对于深入贯彻落实，党中央决策部署，总体国家安全观和习近平总书记，对密码工作的指示要求、更好地发挥密码在保护国家安全，促进经济社会发展，保护人民群众利益方面的重要作用，具有十分重要的意义。国家密码管理局将认真贯彻落实密码法，全面履行密码法赋予的各项职责，坚持党管密码和依法管理的有机统一，确保这部法律宣传到位、贯彻到位、落实到位。”

密码法的出台，使神秘的密码真正进入了公共视野。在网络世界，密码就像一个看不见的安全卫士，无时无刻不在守护着网络与信息安全。贯彻实施密码法，努力提高全社会密码安全意识，营造尊法、学法、守法、用法的浓厚氛围，是各级政府和全社会的共同责任。（来源：央视焦点访谈）

➢ 筑牢个人信息安全防火墙

移动互联网时代，手机 App（应用程序）已成为我们生活中不可或缺的重要部分。然而与此同时，一些 App 违规、越权收集和使用用户个人信息的问题依然突出。

App 违规收集个人信息

对于不少手机用户来说，手机 App 泄露个人信息是“防不胜防”的大难题。去年发布的

《App 个人信息泄露情况调查报告》中就曾指出，逾八成受访者遇到过个人信息泄露的问题，造成用户个人信息泄露的主因集中于经营者未经授权收集个人信息和故意泄露信息这两项。

明明是拍摄软件，却需要获知个人定位；明明是搜索引擎，也同样需要开启麦克风、摄像头等配件使用权限……诸如此类的权限获取要求，对许多用户来说并不陌生。有些权限请求理由正当，有些则把“越权”的权限请求藏于复杂的隐私协议内容中“打包”提供给用户，利用用户有时不会认真阅读相关协议内容的心理，“稀里糊涂”地便向 App 经营方提供了原本不需开启的权限。

截至去年底，市场上可监测到的 App 总量达 449 万款。海量应用背后，应用市场良莠不齐、鱼龙混杂的情况不容忽视。去年 11 月，中消协就曾发布过《100 款 App 个人信息收集与隐私政策测评报告》，报告指出，在 100 款 App 中有多达 91 款 App 存在过度收集用户个人信息的问题。而像用户的账号、密码、手机号等隐私信息，若是在未经用户许可的情况下经 App 隐蔽收集，将会严重影响用户的财产甚至人身安全。

筑造“防火墙”是场持久战

为有效保护消费者的个人信息安全，今年 1 月，中央网信办等部门发布《关于开展 App 违法违规收集使用个人信息专项治理的公告》，在全国范围内组织开展 App 违法违规收集使用个人信息专项治理。与此同时，中央网信办已陆续起草《数据安全管理办法》《移动互联网应用（App）收集个人信息基本规范》等系列制度文件并公开征求意见。

治理 App 违规收集用户信息究竟还存在哪些难点？中国政法大学传播法研究中心副主任朱巍表示，现阶段，整治手机 App 越线违规收集用户信息的问题难点之一在于技术，因有时无法准确判断 App 到底搜集到了用户的哪些信息。“究竟把我们的信息收集到了什么程度，

这其中必要性和正当性的范围是什么。如果所有的信息搜集用户都能够看得到、都知道去哪儿了，那将是很好的保护。”

筑造用户信息安全的“防火墙”是一场持久战，需要政府、平台等多方形成合力，共同营造良好的 App 使用环境。朱巍表示，应推动个人信息保护法的出台，但也要注意保护的“度”，平衡多方关切。“个人信息保护法的出台，并不是与互联网完全断绝关系，‘过度保护’也不行。要将产业发展的未来、技术应用权与用户安全之间的关系处理好，在充分调研、广泛征求意见的基础上出台个人信息保护法。”

若想切实保护用户信息安全，需要通过个人信息保护法加强对违法违规行为的追究，提高 App 运营方的违规成本。专家指出，对于 App 运营公司来说，哪些信息可以获得、哪些信息不应越权，这同样需要制定统一的国家标准，仅靠行业自律很难实现。

朱巍同时建议，用户使用 App 时要学会保护好个人的隐私信息，在自己的手机终端做好最后一道“守门人”。“一是要在正规的应用商店下载 App；二是在进行敏感信息授权时要注意，比如说 App 想要访问通讯录、访问微信等，除非对这个 App 非常信任、对功能非常需要，否则一般不要同意、不要授权。”朱巍说。（来源：人民日报海外版）

➢ 解读《App 违法违规收集使用个人信息行为认定方法》

伴随着互联网大数据产业的快速发展，对个人信息安全的监管也逐步加强。自 2019 年 1 月至 12 月，监管部门在全国范围内组织开展 App 违法违规收集使用个人信息专项治理工作，专项整治的 App 范围涵盖了电子商务、地图导航、快递外卖、交通票务等多方面。2019 年 12 月 20 日 App 专项治理工作组发布了《关于 61 款 App 存在收集使用个人信息问题的通告》（下称“《通告》”），针对 7 月至 10 月间开展 App 评估工作中发现的关于收集使用个人信息问题情况进行通告。

从该通告附表中所列各 App 存在问题来看，47 款 App 存在“申请打开可收集个人信息权限时未同步告知用户其目的”问题；46 款 App 存在“既未经用户同意，也未做匿名化处理，通过客户端嵌入的 SDK 向第三方提供个人信息”问题；34 款 App 存在“未逐一列出嵌入的第三方 SDK 收集使用个人信息的目的、类型”问题。由此可见当前的检查不仅局限于隐私政策、用户提示及告知方式等层面，还涉及到内嵌 SDK 个人信息传输、匿名化处理等后台乃至技术层面检查。因此，如何对 App 个人信息收集使用进行合规体系建设，如何有效实现

产品合规成为运营者需要首先关注的问题。

正文：2019 年 12 月 30 日由国家互联网信息办公室秘书局、工业和信息化部办公厅、公安部办公厅、市场监管总局办公厅联合发布的《App 违法违规收集使用个人信息行为认定方法》（下称“《认定方法》”），被认为会成为监管机构执法的重要参考依据，起到了监管规范具体落地的功能。其中的认定标准为具体的合规工作划出了红线，在此我们结合法规及实践对《认定方法》进行逐条解读，以期为运营者在合规工作中提供有效参考。

一、以下行为可被认定为“未公开收集使用规则”

1.在 App 中没有隐私政策，或者隐私政策中没有收集使用个人信息规则；

解读：经过近一年多来的整顿，市场教育已经取得明显成效，不考虑隐私政策内容是否完善的情况下，大部分 App 会匹配单独的隐私政策，但是也有个别 App 无视监管要求，仍旧裸奔。

2.在 App 首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；

解读：请注意本条款要求的“首次运行”，这里的首次运行不是首次注册、首次登录、或首次交易，意即，当用户首次打开 App 时，就应该向用户展示隐私政策，在获得用户授权同意的情况下，方可收集用户的个人信息。我们可以看到，部分头部 App 在用户一打开 App 时，即弹出隐私政策，通过隐私政策先行的方式获得用户的授权。

3.隐私政策等收集使用规则难以访问，如进入 App 主界面后，需多于 4 次点击等操作才能访问到；

解读：除了在打开 App 时，弹出隐私政策让用户点击同意外，用户希望在其他时间节点也可以顺利访问隐私政策，但是不同的 App 会通过不同的路径展示隐私政策，有时候会对用户的访问造成一定的障碍。最常见的访问路径为我→设置→隐私/关于 XX→隐私政策。我们建议 App 按照主流路径安排隐私政策的访问位置。

4.隐私政策等收集使用规则难以阅读，如文字过小过密、颜色过淡、模糊不清，或未提供简体中文版等。

解读：我们建议隐私政策使用与 App 页面同样字体、颜色及字号大小的文字，上下字号差不超过 1，使用适当的行距及段落间距，对于标题、专有名词、个人敏感信息、提醒用户注意、增加用户责任等内容加粗或用下划线表示。

二、以下行为可被认定为“未明示收集使用个人信息的目的、方式和范围”

1.未逐一列出 App(包括委托的第三方或嵌入的第三方代码、插件)收集使用个人信息的目的、方式、范围等；

解读：第三方代码、插件有两种性质，第一种不在 App 上露出，不单独向用户获得授权，用户难以感知，根据《信息安全技术个人信息安全规范》8.6 条的注释部分，该类第三方代码、插件与 App 属于共同个人信息控制者，用户无从约束该类第三方代码、插件，只能通过约束 App 来间接实现对该类第三方代码、插件的约束，当然，相应的约束责任也应该由 App 来承担。

第二种会与用户进行交互，单独向用户获得授权，根据《信息安全技术个人信息安全规范（征求意见稿）》8.7 条，该类第三方代码、插件属于接入第三方，App 可以通过事前评估、记录、协议约定、审计等措施来约束该类第三方代码、插件。从本条要求来看，此处的第三方代码、插件并不在 App 上露出，需要 App 明示该等第三方代码、插件的身份以及收集使用个人信息的目的、方式和范围等。根据监管要求，App 应按照业务功能的划分逐项说明个人信息的收集使用规则，各项业务功能与所收集个人信息目的、范围应该是一一对应的关系。

2.收集使用个人信息的目的、方式、范围发生变化时，未以适当方式通知用户，适当方式包括更新隐私政策等收集使用规则并提醒用户阅读等；

解读：何为“适当方式”，《App 违法违规收集使用个人信息自评估指南》评估点 18 指出，App 应通过电子邮件、信函、电话、推送通知等方式告知用户并提醒用户阅读；而《信息安全技术个人信息告知同意指南（草案）》8.2f):宜使用弹窗、浮窗、短信、邮件、消息推送等显著方式进行告知。

很明显，弹窗、浮窗的告知效果更好，其他方式都存在无法有效告知的情形，但是频繁

的弹窗、浮窗又会影响用户体验，我们建议在收集使用规则发生重要变化时，宜使用弹窗、浮窗的告知方式并获得用户同意，其他变化诸如个人信息保护负责人联络方式的变化等，可通过其他途径告知。

3.在申请打开可收集个人信息的权限，或申请收集用户身份证号、银行账号、行踪轨迹等个人敏感信息时，未同步告知用户其目的，或者目的不明确、难以理解；

解读：在用户打开 App 后展示隐私政策前，一些 App 通过弹窗的形式要求获得用户手机号码、IMEI、IMSI 权限，设备定位权限以及访问照片、媒体内容和文件的权限等，该等弹窗并未明示收集信息的目的或目的难以理解，以至于用户在点击“允许”的时候产生诸多质疑。在近期 APP 专项治理工作组发布的《关于 61 款 App 存在收集使用个人信息问题的通告》中，获取用户权限时，未同步告知用户目的的多家 App 被曝光。我们建议，App 在申请个人信息收集权限以及获取用户敏感信息时，通过弹窗、浮窗或小字标注的方式告知用户收集目的，而不是仅仅在隐私政策中说明。

4.有关收集使用规则的内容晦涩难懂、冗长繁琐，用户难以理解，如使用大量专业术语等。

解读：从模仿跨国公司的隐私政策，到逐渐形成自有表述体例，隐私政策的内容及表述方式已经落地很多，大大减少了用户的阅读阻力，尤其是专项治理以来，头部企业的隐私政策文本不断调整完善，为全行业提供了可供参考的模板。建议还未满足本要求的 App，可以参考头部企业的隐私政策文本，并将本平台特有的专业内容进行细化简化，提供符合一般大众理解水平的内容。同时，对于需要详细解释的定义、场景等，可以通过链接的方式在跳转页面进行更进一步的解释说明。

三、以下行为可被认定为“未经用户同意收集使用个人信息”

1.征得用户同意前就开始收集个人信息或打开可收集个人信息的权限；

解读：部分 APP 在用户授权同意收集个人信息前即开始收集设备标识符、位置、浏览记录等信息，此时的收集未获得用户同意，显然违反了《网络安全法》第四十一条的规定；本条要求与 1.2 条要求近似，意即，应在用户首次打开 App 时，提示用户阅读隐私政策及获取收集权限。我们建议在用户打开 App 后，及时弹出隐私政策弹窗或链接，提醒用户阅读隐私政策内容并获取用户的授权同意，同理，App 应通过弹窗方式告知用户申请权限的目的并获取用户的授权同意，在用户未确认同意前或拒绝同意后，App 不应收集用户的个人信息。

2.用户明确表示不同意后，仍收集个人信息或打开可收集个人信息的权限，或频繁征求用户同意、干扰用户正常使用；

解读：用户未点击同意按钮，或者点击拒绝按钮，或者关闭展示的授权弹窗可视为用户明确表示不同意，此时如 App 无视用户意愿仍旧收集个人信息或擅自打开收集权限，属于未征得用户同意的收集行为，已然违反了相关法律规定。

部分 App 在用户明确表示不同意后，频繁弹出弹窗征求用户同意，对于“频繁”的界定可参考《信息安全技术移动互联网应用（App）收集个人信息基本规范（草案）》4.1f):48 小时内超过一次即视为“频繁”。

3.实际收集的个人信息或打开的可收集个人信息权限超出用户授权范围；

解读：这是实践中非常普遍的问题，隐私政策展示的收集使用规则及授权收集权限与 App 的实际收集使用情况不相符。通常有两种情形，一种是隐私政策中未说明某项功能或场景的收集使用目的、范围，而 App 擅自收集；一种是隐私政策对某项功能或场景收集使用规则进行了说明，但是 App 实际收集的个人信息超出了说明范围。

个人信息收集日志可以实现对个人信息收集过程的可追溯，也是监管执法的重要依据，建议 App 建立个人信息收集日志，严格按照授权范围收集个人信息，如超出授权范围，应再次征得用户的授权同意。

4.以默认选择同意隐私政策等非明示方式征求用户同意；

解读：截止到目前，仍有相当 App 通过“登录即同意《隐私政策》”、“继续使用即同意《隐私政策》”，以及默认勾选的方式征得用户同意。《App 违法违规收集使用个人信息自评估指南》评估点 24 指出：用户主动填写、点击、勾选等自主行为，作为产品或服务的业务功能开启或收集个人信息的条件。隐私政策须通过明示方式征得用户同意，建议 App 通过用户的主动点击、勾选等自主行为来获得用户的授权同意。

5.未经用户同意更改其设置的可收集个人信息权限状态，如 App 更新时自动将用户设置的权限恢复到默认状态；

解读：未经用户同意更改其设置的可收集个人信息权限状态，可视为违背用户意愿，欺瞒用户，未获得用户授权同意而擅自收集个人信息，已然违反征得用户同意的前置原则。

6.利用用户个人信息和算法定向推送信息，未提供非定向推送信息的选项；

解读：定向推送，即精细化运营，可以显著提升 App 的运营效率，但是定向推送也会产生一些负面效应，比如影响用户体验，愚民愚智效果，歧视差别对待等，App 应该给予用户非定向推送信息的选择。但是实践中，提供选项容易，用户找到选项不易。

我们建议，App 应将选项设置在合理位置，避免用户难以实现选择权，比如美团的路径为“我→设置→通用→隐私管理→接受个性化推荐”；再如饿了么的路径为“我→设置→通

用→个性化推荐设置”。

7.以欺诈、诱骗等不正当方式误导用户同意收集个人信息或打开可收集个人信息的权限，如故意欺瞒、掩饰收集使用个人信息的真实目的；

解读：评估是否属于“不正当”，建议从 1.是否通过“等”“合作方”“业务需要”等概括表述方式进行掩饰，2.是否使用含糊明显有歧义的收集使用规则误导用户，3.是否通过虚假收集使用规则欺骗用户；4.是否通过虚假利益诱导用户授权等几个方面来考量。

8.未向用户提供撤回同意收集个人信息的途径、方式；

解读：此处的撤回应指部分个人信息的撤回，部分个人信息的撤回包括部分业务功能对应的个人信息的撤回也包括单一业务功能中部分个人信息的撤回。

淘宝的隐私政策对于改变授权同意的范围及路径进行了概要性表述，微信的隐私政策将撤回同意拆分为八个业务功能并同时告知撤回路径，八个业务功能包括关闭推荐通讯录朋友、关闭附近的人设置、关闭微信运动、关闭摇一摇、删除微信支付银行卡、撤回向其他应用的信息授权（全部）、撤回向其他应用的信息授权（部分）、在微信游戏撤回向其他应用的信息授权（部分）。我们建议 App 可以按照业务功能划分向用户提供撤回授权同意的路径，也可以按照个人信息的类型和范围划分向用户提供撤回授权同意的路径。

9.违反其所声明的收集使用规则，收集使用个人信息。

解读：本条系 App 披露的收集使用规则与实际收集使用规则不一致，前面已有评述，此处不赘述。

四、以下行为可被认定为“违反必要原则，收集与其提供的服务无关的个人信息”

1.收集的个人信息类型或打开的可收集个人信息权限与现有业务功能无关；

解读：XX 天气 App 曾因收集位置信息以外的个人信息而被曝光，App 的业务功能应与所收集个人信息类型一一对应，意即，所收集的个人信息类型应是满足对应业务功能运转的最少必要信息，与业务功能完全无关的个人信息当然不能成为 App 收集的范围。

我们建议评估个人信息是否与业务功能相关应该从 1.不收集该个人信息，业务功能无法有效运转；2.不收集该个人信息，App 或该项业务功能有很大运营风险（包括安全风险、法律风险等）；3.为符合监管要求所必须收集等几个方面进行考虑。

2.因用户不同意收集非必要个人信息或打开非必要权限，拒绝提供业务功能；

解读：必要信息的概念可以参考《信息安全技术个人信息安全规范》5.2a):没有上述个人信息的参与，产品或服务的业务功能无法实现。必要信息的范围可以参考《信息安全技术移动互联网应用（App）收集个人信息基本规范（草案）》附录。

App 收集非必要信息以及打开非必要权限需要获得用户的明示同意，在用户拒绝的情形下，为了避免合规风险，App 仍须提供该等业务功能，除非 App 有合理理由（是否合理可以参照行业惯例）证明该等个人信息属于必要信息。

3.App 新增业务功能申请收集的个人信息超出用户原有同意范围，若用户不同意，则拒绝提供原有业务功能，新增业务功能取代原有业务功能的除外；

解读：如新增业务功能可以和原有业务功能并存，则用户有权同意是否授权新增业务功能收集个人信息，App 不应拒绝提供原有业务功能；如新增业务功能取代原有业务功能，用户不同意授权新增业务功能收集个人信息的，App 有权拒绝提供原有业务功能以及新增业务功能。此处的“取代”可以理解为原有业务功能不存在，如果是部分取代，还需要根据具体场景进行分析。

4.收集个人信息的频度等超出业务功能实际需要；

解读：根据《信息安全技术移动互联网应用（App）收集个人信息基本规范（草案）》2h)：App 应以实现服务所必需的最低合理频率向后台服务器发送个人信息。这两份文件中的“频度”指的不是一回事儿，一个指收集频度，一个发送频率。差别原因在于不是所有 App 收集的个人信息都需要向后台服务器发送，有些缓存信息，当用户关闭 App 后即清除，App 后续也无法使用这些不存储在设备中的缓存信息，对个人信息主体造成的影响就非常有限。

但是此处仅指收集频度，比如，某 App 为了提供服务必须收集位置信息，如果频繁收集且同时回传后台服务器，该位置信息就会转化为行踪轨迹，而行踪轨迹属于个人敏感信息范畴，该类信息会对个人信息主体的人身、财产、名誉等产生重大影响。意即，收集的频度会转化个人信息的类型或范围，所以收集频度也属于 App 需要注意的合规考量因素。

5.仅以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，强制要求用户同意收集个人信息；

解读：从本条要求可以看出，改善服务质量、提升用户体验、定向推送信息、研发新产品等明显不属于基本业务功能，是否属于业务功能仍有争议，所以句首使用了“仅”，同时，本条突出了“强制”，意即，如果用户自主同意基于该等目的收集信息的，App 仍可以收集，但是用户不同意的，App 不得强制收集或拒绝提供业务功能。

6.要求用户一次性同意打开多个可收集个人信息的权限，用户不同意则无法使用。

解读：这里使用了“一次性”“多个”，我们理解这里的个人信息权限包括了非必要权限，如果是一次性打开必要权限且告知收集使用目的和范围，我们认为用户不同意的情况下 App 有权拒绝提供业务功能；如用户同意必要权限不同意非必要权限的，App 并不能拒绝提供业

务功能；且 App 不应将非必要权限与必要权限进行捆绑要求用户同意非必要权限。

五、以下行为可被认定为“未经同意向他人提供个人信息”

1.既未经用户同意，也未做匿名化处理，App 客户端直接向第三方提供个人信息，包括通过客户端嵌入的第三方代码、插件等方式向第三方提供个人信息；

解读：从本条“既”“也”的表述可知，征得用户同意的，App 客户端可直接向第三方提供个人信息；个人信息经过匿名化处理的，App 客户端也可直接向第三方提供个人信息；两者都未进行的，就属于违法提供。个人信息经过匿名化处理后，不能再次识别到特定个人，即，经过匿名化处理的个人信息不再属于个人信息，App 客户端对外提供不会违反关于个人信息保护的相关监管要求。

在 APP 专项治理工作组发布的 57 款存在收集使用个人信息问题的通告中，违反本条的通报 App 达到 46 款，尤其是通过客户端嵌入的第三方代码、插件向第三方提供用户的个人信息的情形非常普遍。

根据《信息安全技术个人信息安全规范（征求意见稿）》8.6 可知，嵌入的第三方代码、插件与 App 形成共同个人信息控制者。如 App 未向用户明确告知第三方代码、插件的身份，以及在个人信息安全方面 App 和第三方代码、插件应分别承担的责任和义务，App 应承担因第三方代码、插件引起的个人信息安全责任；在 App 通过第三方代码、插件向第三方提供个人信息时，由于第三方代码、插件并不直接与用户交互，只能通过 App 向用户获得收集使用的授权。我们建议，App 应向用户明确告知第三方代码、插件的身份，以及双方分别承担的权责义务，除此之外 App 客户端直接或通过第三方代码、插件向第三方提供个人信息时还应获得用户的授权同意或者对个人信息进行匿名化处理。

2.既未经用户同意，也未做匿名化处理，数据传输至 App 后台服务器后，向第三方提供其收集的个人信息；

解读：此处的“提供”应指共享、转让，不包括委托处理的情形，根据《信息安全技术个人信息安全规范（征求意见稿）8.1，委托处理场景下，App 在授权范围内向受托人提供个人信息的，无需额外获得用户的授权同意。在进行共享转让的场景下，App 应对接收方进行安全影响评估；还需向用户告知共享转让目的、接收方身份，并事先取得用户对于共享转让的授权同意；同时，App 与个人信息接收方应记录并保存共享转让情况。

3.App 接入第三方应用，未经用户同意，向第三方应用提供个人信息。

解读：在 App 客户端使用接入第三方应用时，App 往往需要向第三方应用共享用户头像、昵称、性别、地区等信息。该个人信息的共享行为需要事先获得用户的授权同意。即，

App 应在告知用户共享个人信息的目的、接收方的类型以及可能产生的后果后，获得用户对于共享个人信息的授权同意。

常规来说，点击第三方应用时，第三方应用会弹出申请授权的窗口，展示申请授权的个人信息范围，用户可点击同意或允许按钮进行授权。该点击行为包括用户同意 App 将其个人信息共享给第三方应用以及同意第三方应用收集其个人信息两层含义。我们建议，网络运营者对接入其平台的第三方应用，应明确数据安全要求和责任，督促监督第三方应用运营者加强数据安全管理。在共享个人信息时，应获得用户的授权同意。

六、以下行为可被认定为“未按法律规定提供删除或更正个人信息功能”或“未公布投诉、举报方式等信息”

1.未提供有效的更正、删除个人信息及注销用户账号功能；

解读：该条要求 App 为用户提供相应的实现对个人信息的访问、更正、删除以及注销账号功能。在实践中，许多 App 未提供该类功能，或者在隐私政策中对此有所描述，但在用户进行操作时无法找到对应功能操作界面，甚至有些 App 客服向用户告知“功能加速开研发中，待上线后处理”等。前述此类设置和处理方式都存在被认定为违法违规行为而存在风险。

结合本条内容及监管要求，我们建议合规工作需考虑两方面内容：第一，在隐私政策中详细向用户说明具体操作步骤（根据《APP 违法违规收集使用个人信息自评估指南》要求，建议实际步骤少于四步。）第二，在应用操作层面对前述功能加以实现，或设置专人负责该类用户诉求。

2.为更正、删除个人信息或注销用户账号设置不必要或不合理条件；

解读：该条要求在提供用户更正、删除及注销操作功能时不得故意设置操作障碍。特别是涉及到注销功能时，由于担心用户流失，一些运营者设计了种种“关卡”以达到降低用户注销率的目的。常见的具体形式包括隐藏该类操作入口、要求用户提供多种证明材料、提示由于捆绑多款其他应用账号而不得注销等。结合监管案例来看，要达到合规要求，本条认定内容需要对“不合理条件”的范畴进行明确。

换言之，设置前提条件并非不可，但需要在合理范围内。如某金融 App 为了账户安全，防止羊毛党利用注销机制反复刷单，攫取不正当利益，因而设置了注册时间不满 1 个月不得注销的条件，获得 App 治理工作组的认可。因此，在设置注销流程时，从保障用户账户安全的角度或维护交易环境安全方面考虑，设置必要核验步骤是合法合规的。但相应的，运营者应当向用户作出简明易懂的规则说明。

3.虽提供了更正、删除个人信息及注销用户账号功能，但未及时响应用户相应操作，需

人工处理的，未在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）完成核查和处理；

解读：该条对运营者针对用户更正、删除信息以及注销账号需求的响应时间提出了要求。尽管目前针对上述核查和处理工作的完成标准尚未明确，但运营者应在用户感知角度及时提供积极反馈信息以达到合规标准。此外，由于不同行业存在差异性，在一刀切的时间要求上是否后续会根据行业进行细化或调整，有待监管进一步实践探索。但从运营者合规角度来说，我们建议对用户的上述功能需求以 15 个工作日为限进行处理。若由于突发情况或意外导致超期的，建议及时对用户进行进度及情形告知并积极保留合规工作痕迹。

4.更正、删除个人信息或注销用户账号等用户操作已执行完毕，但 App 后台并未完成的；

解读：该条内容的主要目的是为防止 App 运营者采取欺骗用户的表面合规而实质违法违规行为。由于用户更正个人信息后 App 是否对此进行响应可以被用户直接感知，因此实践中主要问题集中在删除个人信息及注销账号操作中。

我们建议，运营者对此除了需要在隐私政策中进行后台操作说明外，还需要在后台操作完毕后向用户给予反馈信息。此外，用户提出前述要求的，如运营者需要存储或使用数据的，建议进行匿名化处理（设置为不可访问状态）并向用户进行说明。

5.未建立并公布个人信息安全投诉、举报渠道，或未在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）受理并处理的。

解读：该条内容是本部分内容的执行保障要求。具体来说，投诉举报渠道是上述 4 条乃至整体用户个人信息处理合法合规的最后一道由运营者提供的安全屏障。因此，为了避免流于表面，该条要求对用户的投诉及举报应当及时（最长 15 个工作日）进行受理并处理。从合规角度来看，我们建议运营者在隐私政策中向用户对该类投诉举报渠道进行醒目展示，并设置相应的工作流程及管理制度。

结语：尽管《认定方法》在法律效力上位阶不高，且其中尚存在一定的内容有待监管在实践中进一步解释或调整，但从整体规制框架来看，由行业的快速发展所带来的变化为自上而下施行监管带来了巨大的挑战。因此《认定方法》的出台，为行业运营者的合规工作划定了较为具体的范畴，对互联网及大数据科技产业合法合规健康发展产生了积极作用。可以预见在接下来的一年里，数据及个人信息安全规范体系将逐细化，监管工作也将随之一同深入展开。及时有效对业务进行调整，完善自身合规体系将是行业从业者的优势所在。（来源：数据法盟）

➢ 放宽数据安全治理的视野

作为网络安全的核心，数据安全日益成为数字经济的“风暴之眼”（the eye of storm）。不过，当下对数据安全的治理，多聚焦于技术层面，制度反思与理论建构均有所不足。为此，本文尝试剖析数据安全治理背后的理论脉络，并探索我国未来的可能进路。

一、基于“公司治理”的“数据安全治理”

“公司治理”（corporate governance），在狭义上是指法人所有者对经营者的一种监督与制衡机制，即通过一种制度安排，合理地界定和配置所有者与经营者之间的权利与责任关系；在广义上，其指通过一整套包括正式或非正式的、内部的或外部的制度来协调公司内各主体之间的利益关系，引导、控制和规范相关主体的各项活动，以最大限度地增进公司法人的共同利益。国际标准化组织 IT 服务管理与 IT 治理分技术委员会、国际数据治理研究所（DGI）、IBM 数据治理委员会（IBM DG Council）等机构，均将“数据治理” （data governance）奠定在公司治理的理念之上。

就此而言，“数据治理”意指建立在数据存储、访问、验证、保护和使用之上的一系列程序、标准、角色和指标，以期通过持续的评估、指导和监督，确保富有成效且高效的数据利用，实现企业价值。具体而言，数据治理包括了元数据管理、数据架构设计、数据库管理、

数据安全管理、数据质量管理、主数据管理、数据仓库和企业情报管理、文件管理等诸多内容。

2018 年，Gartner 从数据治理出发，提出了“数据安全治理”（DSG）框架。其指出：数据安全治理不仅仅是一套用工具组合的产品级解决方案，而是从决策层到技术层，从管理制度到工具支撑，自上而下贯穿整个组织架构的完整链条。组织内的各个层级之间需要对数据安全治理的目标和宗旨取得共识，确保采取合理和适当的措施，以最有效的方式保护数据资源。

总之，基于公司治理的数据安全治理，立足于特定企业，在公司内建规立制，通过人员、技术、流程、组织的协调，就数据生命全周期实现数据的安全保护，具有私人性、营利性和管理性的特色。

二、迈向“公共治理”的“数据安全治理”

基于公司治理的数据安全治理固然为数据安全提供了切实可行的操作架构，但它既小觑了“数据”，并窄化了“治理”。

数据不仅仅是企业的投入品，更是国家经济运行机制的重要生产要素，是国家治理能力的“基础性战略资源”，其重要性甚至居于矿藏、土地、河流等耳熟能详的战略资源之上；数据亦不仅仅是企业的产出品，更关乎世界范围内的生产、流通、分配、消费活动，具有全球化和跨国界的天然属性；数据也不仅仅限于企业，在数字化生存的时代，它改变了普罗大众对自我和对隐私的观念，同时塑造了人与人交往的方式。以此观之，既有的数据安全治理挂一漏万，只看到了数据的技术经济维度，而忽略了数据所蕴含的社会性、政治性和国际性的多重面向，“深度伪造”便是典型的例子。Deepfake（深度伪造）作为“deep learning”（深度学习）和“fake”（伪造）的合成词，意指利用人工智能技术实现图像、视频、音频的生成或修改，达到信息内容以假乱真的目的。

与传统对数据泄露的担忧不同，人们对“深度伪造”的批评主要是公共层面的。其首当其冲的就是政治风险和国家安全。在美国，深度伪造多次被用来歪曲知名政治人物的行为和言论。对他人名誉权、肖像权，甚至商誉的侵害是深度伪造的第二罪状。2019 年 6 月，DeepNude 应用发布，只要你提供一张他人的照片，它就可以根据这张照片使用深度伪造技术，还原此人的裸体形象，很快就陷入巨大争议而下线。可以设想，利用“深度伪造”技术能够创造一家上市公司 CEO 宣称公司即将破产的虚假视频，公司股价必将应声而落，其损失难以估量。最后，深度伪造已经成为“社交诈骗”的一部分，人们会误以为收到了来自亲友的消息和指示，遭受精神和金钱的双重损失。

而在上述风险的背后，则是整体信任衰退效应导致的社会信任危机。社会建立的基础不是强制力，而是信任。大量的研究证明：个体与组织之间、组织与组织之间、组织与社会之间的诚信关系及其信任度，已经成为影响个体、组织及社会发展繁荣的关键变量之一。深度伪造的广泛使用，必将造成“假作真时真亦假，无为有处有还无”的困境。当眼见不再为实，耳听更是为虚的情形下，所有人都不得不先抱持怀疑一切的态度，只有在付出辨明真伪的成本和努力之后，才能得到宝贵的信任。正因如此，美国学者 Robert Chesney 和 Danielle Citron 认为深度伪造扭曲民主对话、操纵选举、侵蚀对机构和媒体的信任，并加剧社会分裂。总之，深度伪造威胁最大的不是个体，而是社会系统。

“深度伪造”所暴露的问题，充分说明数据安全已经越过了既有数据安全私人治理的边界，向公共治理迈进。

三、数据安全的“整体治理”

“治理”并不仅仅是公司管理的一部分，相反，它始终关注着公共领域，并力图跨越私营部门和公共机构的二元对峙，最终实现“善治”（good governance）。1995 年，联合国“全球治理委员会”（the Commission on Global Governance）在《我们的全球伙伴关系》中，将“治理”界定为各种公共或私人的个人和机构管理其共同事务的诸多方式之总和，一种使相互冲突的利益得以调和并采取联合行动的持续过程。从“管理”到“治理”，在主体上体现为从“单一主体”向“多元社会经济组织”的转变，在规则上体现为“正式制度”向“契约、行业标准、其他非正式制度”的转变，在向度上体现为从“自上而下”控制向“自上而下或平行运行”协调的转变。

考虑到网络空间的特征，我们不妨用“整理治理”（Holistic Governance）来描述基于公共治理的数据安全治理范式。整体性治理最早由英国约克大学的安德鲁·邓西尔在 1997 年的《整体性治理：新的改革议程》一书中提出。所谓“整体性治理”，即以核心需求为治理导向，以信息网络技术为治理手段，以协调、整合、责任为治理机制，对治理层级、功能、公私部门关系及信息系统等碎片化问题进行有机协调与整合，不断从分散走向集中、从部分走向整体、从破碎走向整合的治理图式。详言之，数据安全的整理性治理有着如下内涵：

（一）治理主体

在复杂的生态系统中，所有的数据利益攸关者都是且应当是数据安全治理的主体，这其中既包括了个人数据主体，也包括了开展数据收集、利用、加工、传输活动的数据业者；既包括了对数据收集、存储、利用和公开负有法定义务的政府机关，也包括了相应的监督管理机构；既包括了形色各异的组织体，也包括了组织体内部直接从事数据处理的组织成员；既

包括了本国政府，也包括其他主权国家和国际组织。

在众多利益相关者之间，整体治理首先要求政府内部的组织创新。通过组织、流程、技术、机制以及政治等一系列制度化路径，其首先促成政府跨不同职能部门之间的协调合作，同时，整体政府通过理顺经济区与行政区的关系来突破区域一体化的发展障碍和制度瓶颈，从而推动了一体化发展。不过，整体性治理并不意味着大块头（one big lump）的政府，它并不完全摧毁职能边界，而是提出职能部门整合的切入点，在不破坏职能分工的专业化的基础上，实现跨边界整合。另一方面，整体治理要求政府与社会组织的协同，将政府、市场和社会三个系统从单方面控制转向多系统协调，发挥各自优势，实现共同的数据安全目标。

（二）治理方式

数据安全的治理方式因治理主体的不同而不同：个人数据主体享有各种权利，法定机关行使权力，监管机构拥有特权，而数据业者和其成员不但有着法定权利，也凭借信息不对称和技术能力获得事实上的控制权。

数据治理并非在真空中开展，任何治理主体的治理活动均受制于美国法学家 Lawrence Lessig 所描绘的四种力量，即法律、社会规范、市场和代码。当然，事变时移，这里的“法律”不再由单一国家主宰，而演化为彼此竞争的主权之中的国家法以及正在成型的国际法；“社会规范”也因多元的利益和价值而日趋分裂：数据自由还是数据安全？正如我们的社会一样，社会规范正在被打破和重塑；“市场”日趋发达，但却遭遇到平台垄断和数据垄断的迷雾；“代码”依然强大，可更强大的算法及其带来的黑箱却更令人忧虑。但无论如何，这不断变化的四种力量依然划定了数据安全治理的边界，我们必须在法律、社会规范、市场和代码的整体性架构下思考数据安全治理。

四、数据安全整体治理的实践：安全数据共享

当前，网络攻击日益频繁，复杂度也与日俱增，为此，企业、个人和政府机构必须充分利用集体知识、经验和能力，更全面地了解所面临的威胁。安全信息在各利益相关方之间的共享，恰恰是提升网络防护能力的重要途径，此即“数据驱动安全”之真意。按照共享主体的不同，我们可将数据共享分为三个层面：

其一，企业与用户之间的数据共享。实时在线的安全软件协助企业与用户不间断地发生着数据交换：对用户而言，他们可以随时连接到企业服务器上，以便下载具有网络欺诈内容和恶意软件网站的最新黑名单列表，帮助其快速识别并清除新型木马病毒以及钓鱼、挂马的恶意网页；对企业而言，用户终端里的大量数据也会上传到云端，企业据此建立全面的软件信息数据库，发现可疑样本，并改善数据安全服务。

其二，企业与企业之间的数据共享。在新的网络安全形势下，融合监测、感知、预警、响应等不同功能的“安全态势感知”，是实现数据安全威胁防范、内控治理的有效模式。作为动态、准实时的预测系统，安全态势感知依赖于对数据的编译、处理和融合，并依此判断变动及发展趋势。为此，不同企业之间的安全数据共享是其建立的前提。未来的《数据安全法》可以在《网络安全法》第 29 条、39 条基础上，进一步拓展安全数据共享的对象和主体范围。在具体制度设计上，可以借鉴美国 2015 年《网络安全信息共享法》，将“安全数据”细化为安全事件、威胁、漏洞、缓解措施、情景感知、最佳做法、战略分析。通过搭建一个既有中心企业又有分布式节点的“混合式共享结构”，要求各方尽量统一数据和接口标准，并适当豁免数据共享的责任，即在各方提供防止、调查或减轻数据安全威胁的协助时，只要符合法律规定的共享要求，便可免于未经信息主体授权或反垄断法下包括“垄断协议”在内的责任。

其三，企业与政府之间的数据共享。各网络强国均十分重视网络安全领域的政企合作。例如，澳大利亚《网络安全战略》中的“企业—政府伙伴关系”旨在鼓励政府与企业共同促进关键基础设施、网络、产品和服务领域的安全。美国 2015 年《网络安全信息共享法》和《国家网络安全保护促进法》同样意在推动联邦政府和企业之间的数据共享。由于企业和政府的不对等性，《数据安全法》可以采取分而治之的手段，一方面，鼓励而非强制企业向政府共享安全数据，除非该等数据将危及国家主权、公众权利和公共利益。另一方面，应强制要求政府将其掌握的安全数据与企业及时共享，除非数据涉及国家秘密或公民隐私。同时，为了解除企业共享数据的后果之忧，政府应承诺数据使用的目的和边界，保护其中的知识产权和商业秘密，适当豁免企业对个人信息保护责任。在特定场合下，若企业主动披露未被政府掌握的安全事件及其数据，可以酌情减轻行政处罚。

随着世界全球化的深入和数字化转型，数据安全已成为国际社会所面临的共同责任。在层出不穷的网络黑客攻击、网络犯罪、网络恐怖主义等挑战面前，没有哪个国家能够置身事外、独善其身。为此，未来的数据安全治理，必将打破民族国家的藩篱，通过国际组织和国家间协作，逐步整合成跨国的多层次治理结构。我国政府应以“网络空间命运共同体”为指针，深度参与数据安全国际治理的进程，推动亚太经合组织等框架下数据安全合作，共同铸就数据安全的全球规则体系。（来源:《中国信息安全》杂志 2019 年第 12 期）

四、政府之声

➢ 国家网信办等部门印发《App 违法违规收集使用个人信息行为认定方法》

2019 年 12 月 30 日，中国网信网公布了关于印发《App 违法违规收集使用个人信息行为认定方法》（简称：《方法》）的通知。

通知显示，根据《关于开展 App 违法违规收集使用个人信息专项治理的公告》，为认定 App 违法违规收集使用个人信息行为提供参考，落实《网络安全法》等法律法规，国家互联网信息办公室、工业和信息化部、公安部、市场监管总局联合制定了《App 违法违规收集使用个人信息行为认定方法》。

此次正式发布的《App 违法违规收集使用个人信息行为认定方法》有六个要点，分别详细介绍了可被认定为“未公开收集使用规则”的行为，可被认定为“未明示收集使用个人信息的目的、方式和范围”的行为，可被认定为“未经用户同意收集使用个人信息”的行为，可被认定为“违反必要原则，收集与其提供的服务无关的个人信息”的行为，可被认定为“未经同意向他人提供个人信息”的行为，以及可被认定为“未按法律规定提供删除或更正个人信息功能”或“未公布投诉、举报方式等信息”的行为。（来源：网信中国）

- **关于印发《App 违法违规收集使用个人信息行为认定方法》的通知**
- **全文：**http://www.cac.gov.cn/2019-12/27/c_1578986455686625.htm

➢ 最高人民法院发布《关于民事诉讼证据的若干规定》

2019 年 12 月 26 日，公布关于修改《最高人民法院关于民事诉讼证据的若干规定》的决定，完善民事诉讼证据规则，促进民事审判证据调查、审核、采信乃至民事诉讼程序操作的规范化，保障当事人诉讼权利。

“电子数据是 2012 年民事诉讼法增加的一种新的证据形式。2015 年最高法发布民事诉讼法解释，对于电子数据的含义作了原则性、概括性规定。”最高人民法院副院长江必新说，为解决审判实践中的操作性问题，此次修改决定对电子数据范围作出详细规定，同时规定了电子数据审查判断规则，完善了电子数据证据规则体系。

根据这份修改决定，电子数据包括：

- 网页、博客、微博客等网络平台发布的信息；
- 手机短信、电子邮件、即时通信、通讯群组等网络应用服务的通信信息；
- 用户注册信息、身份认证信息、电子交易记录、通信记录、登录日志等信息；
- 文档、图片、音频、视频、数字证书、计算机程序等电子文件；
- 其他以数字化形式存储、处理、传输的能够证明案件事实的信息。

修改决定规定，人民法院对于电子数据的真实性，应当结合电子数据的生成、存储、传输所依赖的计算机系统的硬件、软件环境是否完整、可靠等 7 类因素综合判断。修改决定同时明确规定，电子数据的内容经公证机关公证的，人民法院应当确认其真实性，但有相反证据足以推翻的除外。

近年来，诉讼中的证据越来越多以电子数据的形式呈现。江必新表示，各级人民法院要密切关注新的信息技术对民事审判工作的影响，加强对电子数据规则适用的研究。要加强对当事人的诉讼指导，积极做好释明工作，加大普法宣传力度，引导当事人正确运用新的证据形式和证明方法完成举证。

此外，修改决定完善了“书证提出命令”制度，扩展当事人收集证据的途径；修改、完善当事人自认规则，更好平衡当事人处分权行使和人民法院发现真实的需要；完善当事人、证人具结和鉴定人承诺制度以及当事人、证人虚假陈述和鉴定人虚假鉴定的制裁措施，推动民事诉讼诚实信用原则的落实。（来源：中华人民共和国最高人民法院）

- **最高人民法院关于民事诉讼证据的若干规定**
- **全文：**http://www.court.gov.cn/fabu-xiangqing-212721.html

➢ 十二部门印发《健康中国行动儿童青少年心理健康行动方案 2019—2022 年》

2019 年 12 月 26 日，国家卫生健康委、中宣部等 12 部门联合印发《健康中国行动——儿童青少年心理健康行动方案（2019—2022 年）》（以下简称《行动方案》）。《行动方案》包括行动目标、具体行动、保障措施三部分。为更好地宣传、贯彻和实施《行动方案》，现就相关内容解读如下。

一、文件出台背景

儿童青少年时期是身心发育的关键时期。开展儿童青少年心理健康工作，对于帮助儿童青少年培养健全的人格、形成自信自强的精神品质、树立理想信念和生活目标都至关重要。世界卫生组织研究发现，精神卫生和心理行为问题（尤其是抑郁症）是年轻人最主要的疾病负担。有些地区调查结果显示，近年来我国儿童青少年心理行为问题发生率和精神障碍患病率逐渐上升，成为重要公共卫生问题。开展儿童青少年心理健康促进，及时预防干预儿童青少年心理健康问题，对个人、家庭、社会都非常重要。党中央、国务院领导同志高度重视儿童青少年心理健康工作，多次作出指示批示，《健康中国行动（2019—2030 年）》心理健康促进行动、中小学健康促进行动都对儿童青少年心理健康工作提出了相关要求。为贯彻落实《国务院关于实施健康中国行动的意见》，推进《健康中国行动（2019—2030 年）》心理健康促进行动、中小学健康促进行动实施，进一步加强儿童青少年心理健康工作，促进儿童青少年心理健康和全面素质发展，国家卫生健康委联合有关部门制订本行动方案。

二、关于行动目标

根据全国各地心理健康服务机构、人员现状及目标可行性，结合《健康中国行动（2019—2030 年）》提出的儿童青少年心理健康相关指标的阶段目标，文件提出了到 2022 年底的行动目标。一方面，从建成心理健康社会环境、形成多方联动服务模式、落实预防干预措施、加强重点人群服务四方面提出总体目标。另一方面，对学校、社区、医疗卫生机构如何建立服务网络提出具体目标。

三、关于具体行动

围绕目标实现，《行动方案》提出了 6 个方面具体行动：一是心理健康宣教行动。媒体、学校、医疗卫生机构对儿童青少年及家长、教师等开展健康教育和科普宣传。二是心理健康环境营造行动。实施“心理滋养 1000 天”行动，营造心理健康从娃娃抓起的社会环境。学校、村（居）委会、妇联、新闻出版、网信等部门营造促进心理健康的校园环境、社区环境、网络环境，倡导家长营造良好的家庭环境。三是心理健康促进行动。学校实施倾听一刻钟、运动一小时“两个一”行动，建立学生心理健康档案，每年评估学生心理健康状况。四是心理健康关爱行动。学校对面临升学压力的学生及家长开展心理辅导，对贫困、留守等学生重点关爱。五是心理健康服务能力提升行动。教育、卫生健康等部门对教师、家长、精神科医师、心理热线工作人员等开展培训，提升服务能力。六是心理健康服务体系完善行动。教育、卫生健康等部门搭建心理健康服务网络，拓展服务内容，完善服务体系。

四、关于保障措施

为确保上述六项具体行动有效落实，文件从加强组织领导与部门协调、保障经费投入、加大科学研究、完善监测评估干预机制四方面提出了相关保障措施。（来源：中华人民共和国国家卫生健康委员会）

- **关于印发健康中国行动——儿童青少年 心理健康行动方案（2019—2022 年）的通知**
- http://www.nhc.gov.cn/jkj/tggg1/201912/6c810a8141374adfb3a16a6d919c0dd7.shtml

➢ 工信部通报下架第一批侵害用户权益 APP 名单

2020 年 1 月 3 日，工业和信息化部信息通信管理局通报：2019 年 12 月 19 日，我部向社会通报了 41 家存在侵害用户权益行为 APP 企业的名单。截至目前，经第三方检测机构核查复检，尚有 3 款 APP 未按要求完成整改（名单见附件）。依据《网络安全法》和《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407 号）等法律和规范性文件要求，我部组织对上述 APP 进行下架。相关应用商店应在本通报发布后，立即组织对名单中应用软件进行下架处理。已经完成整改的 APP，应于 2020 年 1 月 6 日 12 点前，在相关渠道更新整改后的 APP 版本。（来源：工业和信息化部信息通信管理局）

- **下架的应用软件名单（第一批）**
- http://www.miit.gov.cn/n1146290/n1146402/n1146440/c7596945/content.html

五、本期重要漏洞实例

➢ Cisco Data Center Network Manager SOAP API 路径遍历安全漏洞

发布日期：2020-01-02
更新日期：2020-01-03
受影响系统：
Cisco Data Center Analytics Framework < 11.3(1)
描述：

CVE(CAN) ID: CVE-2019-15981
Cisco Data Center Network Manager 是数据中心的网络管理解决方案。
Cisco DCNM 的 SOAP API 中的漏洞可能允许通过身份验证，具有管理特权的远程攻击者在受影响的设备上执行任目录遍历攻击。该漏洞是由于用户提供的 API 输入没有有效的验证，通过向 API 发送精心设计的请求，攻击者可以利用此漏洞读、写或执行任意文件。

<*来源：vendor
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200102-dcnm-path-tr
*>

建议：

厂商补丁：
Cisco

Cisco 已经为此发布了一个安全公告（cisco-sa-20200102-dcnm-path-trav）以及相应补丁：
cisco-sa-20200102-dcnm-path-trav：Cisco Data Center Network Manager Path Traversal Vulnerabilities
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200102-dcnm-path-trav

➢ WordPress WP-Planet rss.class/scripts/magpie_debug.php 跨站脚本安全漏洞

发布日期：2019-12-27
更新日期：2020-01-02
受影响系统：
WordPress WP-Planet <= 0.1
描述：

CVE(CAN) ID: CVE-2014-4592

WordPress 是 WordPress 基金会的一套使用 PHP 语言开发的博客平台。
WordPress WP-Planet 0.1 及之前版本，rss.class/scripts/magpie_debug.php 文件存在跨站脚本漏洞。通过 url 参数，攻击者可利用该漏洞注入任意 Web 脚本或 HTML。

<*来源：vendor
*>

建议：

厂商补丁：
WordPress

目前厂商还没有提供补丁或者升级程序，我们建议使用此软件的用户随时关注厂商的主页以获取最新版本：
http://wordpress.org/
参考：
http://codevigilant.com/disclosure/wp-plugin-wp-planet-a3-cross-site-scripting-xss

➢ Linux kernel cfg80211_mgd_wext_giwessid 缓冲区溢出漏洞

发布日期：2019-10-04
更新日期：2019-12-30
受影响系统：
Linux kernel <= 5.3.2
描述：

CVE(CAN) ID: CVE-2019-17133
Linux kernel 是开源操作系统 Linux 所使用的内核。
Linux kernel 5.3.2 之前版本，net/wireless/wext-sme.c 中 cfg80211_mgd_wext_giwessid 没有拒绝较长的 SSID ID，存在缓冲区溢出漏洞，攻击者利用此漏洞可造成受影响程序崩溃或执行任意代码。

<*来源：vendor
*>
建议：

厂商补丁：
Linux

目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：
https://marc.info/?l=linux-wireless&m=157018270915487&w=2

http://lists.opensuse.org/opensuse-security-announce/2019-10/msg00064.html
http://packetstormsecurity.com/files/155212/Slackware-Security-Advisory-Slackware-14.2-kernel-Updates.html

➢ IBM QRadar 跨站脚本漏洞

发布日期：2019-08-02
更新日期：2019-12-27
受影响系统：
IBM QRadar 7.3.0 - 7.3.2 Patch 4
描述：

CVE(CAN) ID: CVE-2019-4470
IBM QRadar Advisor 是一套安全威胁分析解决方案。
IBM QRadar 7.3.0-7.3.2 Patch 4 版本，在实现中存在跨站脚本漏洞，攻击者可利用该漏洞在 Web UI 中插入任意 JavaScript 代码，从而获取可信会话里的凭证信息。

<*来源：vendor
*>

建议：

厂商补丁：
IBM

目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：
https://exchange.xforce.ibmcloud.com/vulnerabilities/163779
https://www.ibm.com/support/pages/node/1103517

六、本期网络安全事件

➢ 黑客攻击飞机维修网络导致阿拉斯加部分航班取消

2019 年 12 月 23 日，网络黑客发起了一次针对 RavnAir 航空公司的网络攻击，最终导致飞机维修等关键系统关闭，迫使 RavnAir 航空公司取消了在阿拉斯加的一系列航班。KTUU 的一份报告显示，这次恶意网络攻击是在周六被发现的，但是这份报告没有提供发起攻击的黑客具体细节。然而，有 6 家航班被取消，大约有 260 名乘客受到直接影响。

当 RavnAir 航空公司发现攻击之后，它立即采取行动，关闭了飞机维修系统。它表示，所有 Dash 8 飞机的航班都被取消。该公司在一份声明中说：“我们将在未来两天内努力增加航班数量。我们尽可能帮助受影响的乘客改订其他航班。”目前，RavnAir 航空公司正在与 FBI 和网络安全专家合作，以恢复系统并调查网络攻击。

本月早些时候，一名前 Jet2 IT 承包商在访问关键系统并删除数据，导致航空公司网络下线 12 个小时后，被判处 10 个月监禁。该人使用他在公司工作期间获得的凭据，连接到关键系统并删除了所有用户帐户。这位 27 岁男子还设法闯入了 Jet2 首席执行官 Steve Heapey 电子邮件帐户。他的网络攻击造成了 16 万 5 千英镑的损失。（来源：cnBeta）

➢ 首例刑事附带民事公益诉讼案：个人非法获取、提供公民个人信息获刑三年

2019 年 12 月 25 日，徐汇法院宣判该院首起刑事附带民事公益诉讼案。男子徐某因仿冒上海知名官方招考网站等行为套取公民个人信息，最终获刑 3 年，并处罚金 30 万元。同时，法院判令徐某在判决生效后 30 日内，就侵犯公民个人信息的行为，在省级媒体上向社会公众赔礼道歉。

徐某今年 30 岁出头，长期在沪从事 IT 工作。2014 年间，徐某在上海某进修学院工作期间，以该学院的名义设立网站，并负责管理维护。2015 年，徐某从学院离职且在该学院要求终止该网站后，仍然使用该网站直至案发。不仅如此，他还先后以自学考试、成人高考、远程教育等名义设立多个网站，考生在网站报名页面填写姓名、手机号码等信息后，徐某将获取的考生个人信息提供给营利性教育机构招生使用，从中获利。期间，徐某仿冒上海知名官方招考网站，网站从网页排版布局甚至是网站 logo 都与官方网站基本一致。为了达到逼真效果，获取学生信任，假冒网站每日同步发布官网相同的内容，极易混淆和引人误解。他还另设置与该官方网站同名的微信公众号、自媒体账号等，误导公民提供身份信息，严重侵犯了考生的合法权益。

经查，2015 年 12 月至 2019 年 7 月，徐某通过设立的网站获取公民信息共计 8000 余条，并按照培训机构招生成功后收取的学费提成，获利 70 余万元。

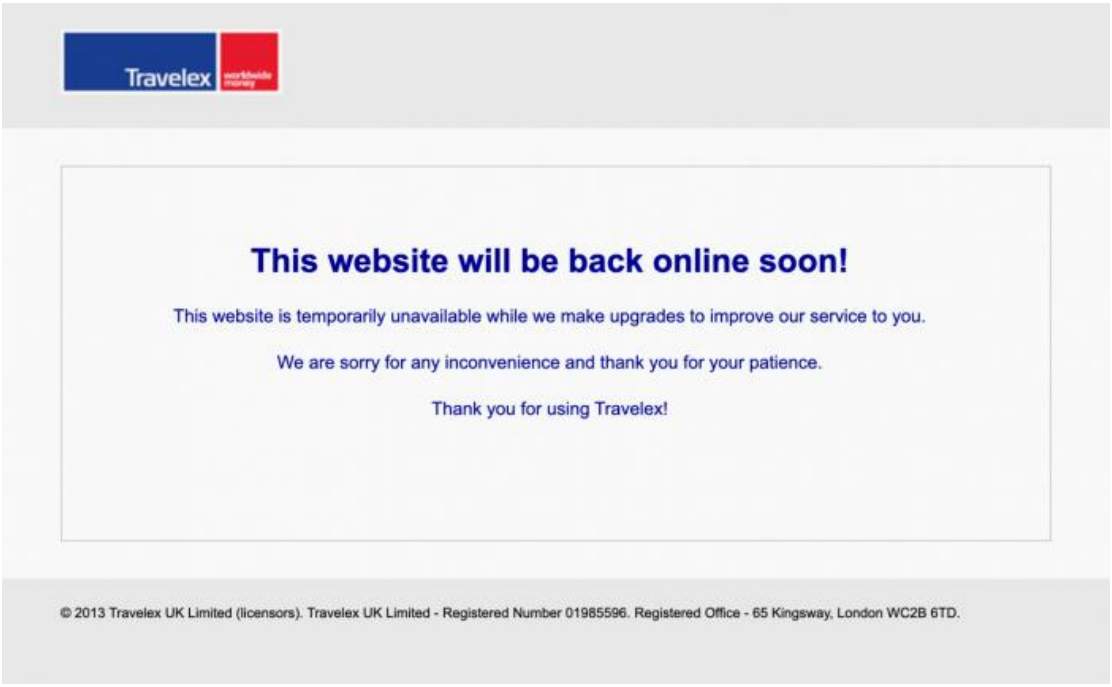
检察机关认为，公民个人信息安全问题已不再停留在个人层面，针对个人信息的违法犯罪活动导致公民的人身、财产、隐私以及正常的工作活动都受到严重威胁，已经上升到整体网络信息安全的重大层面，应当是带有公共利益性质的抽象法益，受我国网络安全法所规制

和保护。为此，检察机关有必要对侵犯公民个人信息安全的行为提起民事公益诉讼。

法院审理后认为，徐某违反国家有关规定，向其他单位提供公民个人信息，其中部分是非法获取，情节特别严重，其行为已构成侵犯公民个人信息罪。同时，徐某侵犯公民个人信息的行为，损害了不特定社会公众的利益，应承担相应的民事责任。法院考虑到徐某自首，且认罪认罚，退出部分违法所得，最终做出上述判罚。（来源：网信上海）

➢ 英国外汇兑换公司 Travelex 因遭到恶意软件攻击暂停服务

2020 年 1 月 3 日，据外媒报道一家大型国际外汇兑换公司证实在 12 月 31 日的时候遭到了恶意软件攻击并由此暂停了一些服务。据悉，这家总部位于伦敦的公司在全球经营着 1500 多家门店。该公司表示，为了保护数据以及阻止恶意软件的进一步传播，作为预防他们将对系统做下线处理。



目前，这家公司的英国网站处于离线状态，当用户登入后会看到“服务器错误”的提示。这家公司网站表示，他们正在升级过程中所以处于离线状态。Travelex 通过官推表示，员工现无法在网站上或通过应用进行交易。据称，一些门店甚至采取手动操作的方式来处理客户的请求。

而像 Tesco Bank 等需要依赖 Travelex 的公司也因此陷入宕机状态。不过 Travelex 指出，截止到目前还没有发现有客户数据遭到泄露，但其并没有就此做详细说明或提供相关证据。

（来源：cnBeta）

➢ 男子给客户提供“翻墙”软件，供其浏览境外网站被警方抓获

2019 年 12 月 23 日，深圳铁路公安处东莞站派出所民警在车站内查获一名提供侵入、非法控制计算机信息系统程序、工具案在逃人员李某。目前，李某已被警方拘留。

深铁警方介绍，嫌疑人李某是湖北省荆门市人。初中毕业后，李某在湖北当地一家职业高中读书，专门学习计算机技术。2016 年，职高毕业之后，李某来到广东东莞务工，在东莞

一家网络公司工作，由于学历不高，加上在职高学习到的计算机技术有限，李某的收入一直不高，所以李某经常会在网上浏览兼职信息。

今年 7 月，李某在网上看到一则招聘信息，浙江省台州市一家“网络公司”招聘技术员，李某通过微信联系上了该公司负责人龚某，龚某简单了解了李某的情况，没有经过面试，也没有办理入职手续，就同意李某入职，并承诺给予李某高额报酬，面对高额报酬，李某并未多想，欣然接受。

随后，龚某向李某介绍了具体的工作内容。原来，龚某的“公司”主要是给客户提供 vpn “翻墙”软件，以供客户浏览境外网站，李某主要负责在网上打广告，同时帮助客户解决技术问题。

深铁警方表示：工信部早已明确规定，未经电信主管部门批准，不得自行建立或者租用 vpn，如果公民私自建立 vpn，并以此牟利达到一定数额或向他人提供软件达到一定人次，均属于情节严重，将受到刑事处罚。而龚某其实并没有注册公司，也未获得电信主管部门审批许可，纯属个人私自租用 vpn 提供给他人使用，李某也因为高额报酬选择铤而走险。

深铁警方介绍，今年 9 月至 11 月，短短两月，李某、龚某就私自租用 vpn 提供给他人使用获利 8 万余元。今年 12 月，台州市公安局网警大队在网络巡查时发现两人的犯罪行为，在台州市成功将龚某抓获，同时将李某列为网逃人员。李某在联系不上龚某后，察觉可能出了问题，便立即更换了手机号码。

12 月 23 日，李某准备一早从东莞乘坐火车前往外地。当天，李某在东莞火车站候车室候车时，深圳铁路公安处东莞站派出所民警发现其神色慌张，行为举止异常。面对警方询问，李某一直不肯说真实姓名，也不愿意出示身份证证件和车票，民警遂将其传唤至派出所接受调查。

深铁警方表示，经过调查，民警最终确定李某就是被浙江省台州市公安局列为网上追逃的嫌疑人。目前，李某已被警方拘留。（来源：深圳日报）

➢ 晒明星乘机记录 国航空乘被停飞

2020 年 1 月 3 日，航空博主“超侧卫”发微博称，自 2019 年 9 月起，名为“若宸”的国航员工多次在个人微博晒出明星的乘机记录，曝光了多位明星的行程及目的地信息。据该博主提供的截图显示，名为“若宸”的用户晒出张杰、邓伦、白敬亭、倪妮等多位明星的

乘机人姓名、生日、国籍等信息，还包括和明星靳东的合影等。

随后，此事引发网友关注。记者注意到，名为“若宸”的微博用户迅速删除了个人微博并更名。当日晚间 10 时 51 分，中国国际航空官博发布声明致歉称，接网友反映，有国航员工个人微博内容涉及旅客信息。经核查，涉事人员系国航一名乘务人员。该员工的行为严重违反了国航数据管理相关规定，目前国航已对该员工作出停飞处分。

据了解，2019 年 7 月，民航局曾发布《关于加强粉丝接送机、跟机现象管理的通知》，其中明确严防民航人员泄露明星乘机信息。针对行程信息泄露，通知提出，民航单位要严防

内部人员进行工作以外的信息查询，禁止利用职务之便泄露知名旅客乘机信息，须签订保密协议。尽管有相关规定，但明星个人信息泄露情况仍频繁发生。记者实测发现，在多个网络平台上仍有大量明星航班信息被公开叫卖。在某社交平台上，搜索“明星姓名+航班”仍然能看到该明星近一两周的航班信息、出行时间等。

2017 年 5 月，最高人民法院、最高人民检察院联合发布的《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》规定，非法获取、售卖或提供个人信息 50 条以上的，即属于“情节严重”。2019 年 2 月，德云社多名艺人住址、行程等信息被多次被泄露、传播及售卖，随后北京市公安局网安总队立即开展侦查并将 3 名嫌疑人抓获。

医疗、房地产等多领域泄密

除航班、住址等信息外，明星就医信息也屡次遭曝光，而且均是内部人员利用职务之便所为。此前，“林俊杰的吊水针头被出售”的话题曾引爆网络。2019 年 10 月某日，林俊杰在结束镇江演唱会后因身体不适，前往镇江第一人民医院就诊。随后歌迷会收到部分截图，显示疑似有个别医护人员擅自在微信群公开就医信息，并在朋友圈发布了林俊杰使用过的吊水针头和药水包照片。其中，部分截图还显示，林俊杰使用过的医疗垃圾疑似未按规定处理，被贩卖后落入他人手中。

随后涉事医院澄清，无医疗废弃物流失，只是追星工作人员拍摄并发在朋友圈的照片被他人转载利用，并且，涉事的 11 名医护人员均被停职半年以上。

据韩媒报道，去年韩国艺人雪莉自杀身亡当日，当地消防灾害总部就泄露了一份雪莉的死亡现场报告书，并在知名社交网站和论坛上流传。随后，该部门向公众道歉，并表示该文件由两名消防员用手机拍摄并发到网上，涉事消防员已被免职。

此外，普通患者信息被内部员工泄露的事件也不在少数。比如，2017 年 2 月，上海 20 万条新生婴儿信息被上海疾控中心、黄浦区疾控中心两名工作人员窃取，并贩卖给婴幼儿保健品经营企业等。

2019 年 4 月到 10 月期间，国家市场监管总局曾开展打击侵害消费者个人信息违法行为专项执法行动，在其公布的 30 个典型案例中，房地产行业包括相关的装修、设计等公司是非法收集、使用个人信息的重灾区，相关案例占比高达 40%。而且均涉及内部人泄密的情况。

事实上，近年来内部人员因职务之便贩卖、泄露个人信息被判刑的案例不在少数。比如，2018 年 6 月，太原市 5 名辅警因通过公安交警综合应用平台非法获取公民个人车辆信息，构成侵犯公民个人信息罪被判刑，其中 1 名主犯被判处有期徒刑三年；2019 年 4 月，河北一名辅警因出售户籍信息、全国车辆驾驶人信息等构成侵犯公民个人信息罪，被判处有期徒

刑六个月，并罚款人民币 2 万元。（来源：南方都市报）

➢ 泰国一监狱闭路系统遭黑客攻击 被放上网络进行直播

2019 年 12 月 27 日，援引外媒报道，泰国南部春蓬府一所监狱的闭路监控电视系统遭到黑客攻击，随后在 YouTube 网站上进行现场直播。目前官方并未公布有关黑客入侵的具体细节，不过当地警方表示是因为收到曾在直播视频中出镜的记者报告才发现的。

根据美联社报道，黑客以 BigBrother’s Gaze 的名字在 YouTube 上进行视频直播，持续了数小时时间。在直播视频中显示了多个安全监控摄像头，由此可以相信黑客可以访问整个监控系统。

泰国当局在随后发表的声明中表示，南部春蓬府 Lang Suan 监狱所属的摄像头系统受到境外黑客攻击而受到损害，但是并没有提供本次黑客攻击行为的更多信息，尚不清楚是谁发起了本次攻击，以及是如何攻入该监狱系统的。

泰国惩教署总干事纳拉特·萨瓦塔南上校表示，在监狱相关官员意识到这个问题之后立即采取了行动，关闭了整个监控系统。目前当地警方已经在调查中。美联社表示，在 YouTube 直播频道中错误的表示这些视频来自于曼谷监狱，但圣诞节当天已经被 YouTube 清理掉了。在撰写本文时，该 YouTube 频道没有任何录像，很可能是帐户所有者删除了该

录像。

该频道写道：“我想向那些可能因我的直播而冒犯的人致歉。事实上这并没有入侵行为，所有摄像头机位均来自于公共领域。附言：可能让你失望的是，该频道可能不会再次出现此类内容。再附言：在安装视频监控器时，请更改标准密码。”（来源：cnBeta）