国盟信息安全通报

2021 年 08 月 30 日第 242 期

全国售后服务中心

国盟信息安全通报

（第 242 期）

国际信息安全学习联盟

2021 年 8 月 30 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 603 个，其中高危漏洞 166 个、中危漏洞 367 个、低危漏洞 70 个。漏洞平均分值为 5.63。本周收录的漏洞中，涉及 0day 漏洞 354 个（占 59%），其中互联网上出现“WordPress 插件 Popular Posts 远程代码执行漏洞、Zoo Management System 'Multiple'跨站脚本漏洞”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原创漏洞总数 12901 个，与上周（3186 个）环比增加 3.0 倍。。

主要内容

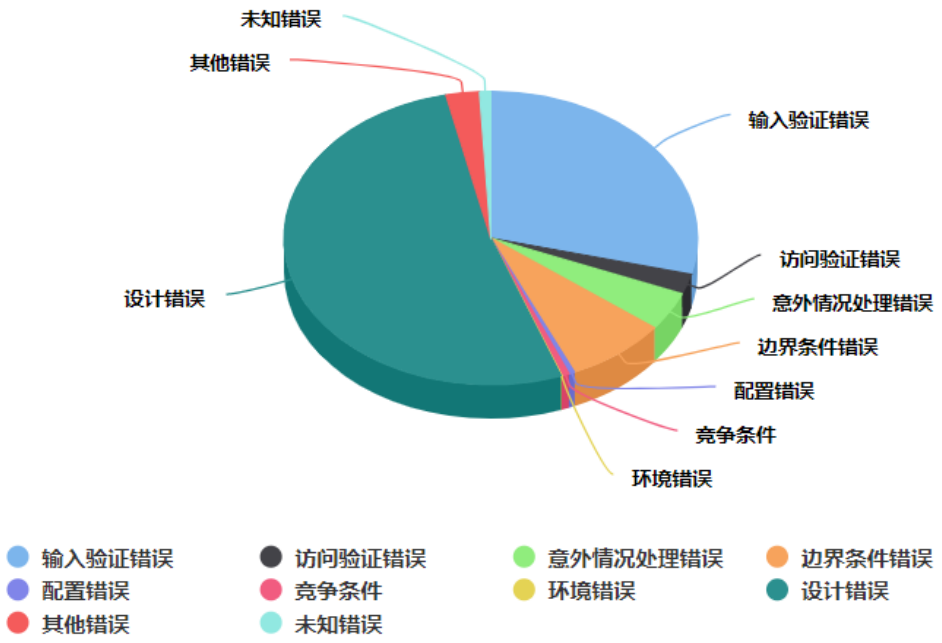
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

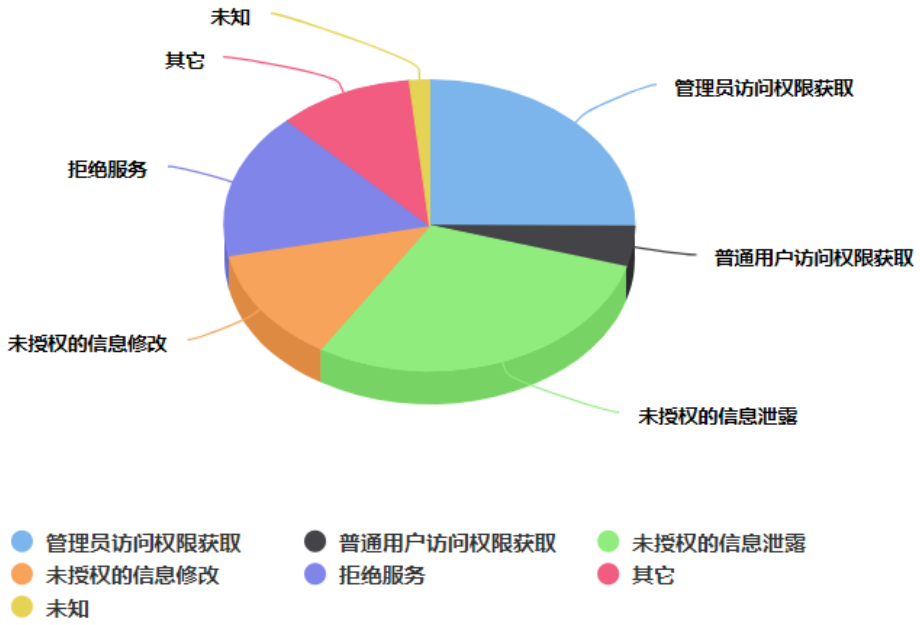
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 603 个，其中高危漏洞 166 个、中危漏洞 367 个、低危漏洞 70 个。漏洞平均分值为 5.63。本周收录的漏洞中，涉及 0day 漏洞 354 个（占 59%），其中互联网上出现“WordPress 插件 Popular Posts 远程代码执行漏洞、Zoo Management System 'Multiple'跨站脚本漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的原创漏洞总数 12901 个，与上周（3186 个）环比增加 3.0 倍。

二、安全漏洞增长数量及种类分布情况

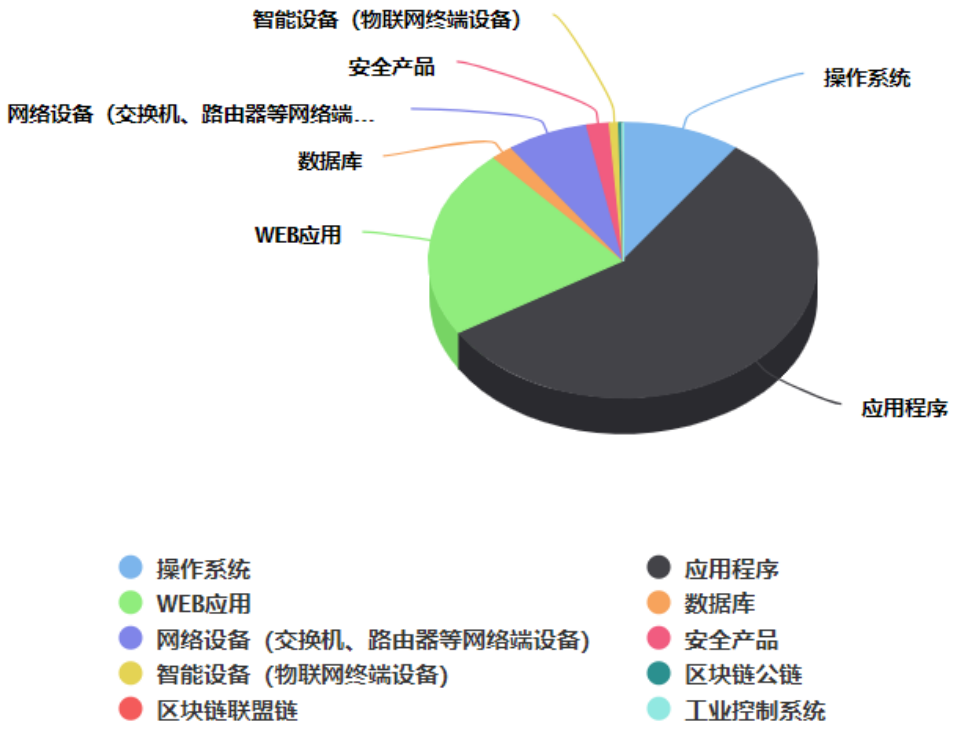
➢ 漏洞产生原因（2021 年 8 月 1 日—2021 年 8 月 30）



➢ 漏洞引发的威胁（2021 年 8 月 1 日—2021 年 8 月 30）



➢ 漏洞影响对象类型（2021 年 8 月 1 日—2021 年 8 月 30）



三、安全产业动态

➢ 解读个人信息保护法十大亮点

2021 年 8 月 20 日，经过三次审议，十三届全国人大常委会第三十次会议表决通过了个人信息保护法，将于 2021 年 11 月 1 日起施行。在信息化时代，个人信息保护已成为广大人民群众最关心最直接最现实的利益问题之一。个人信息保护法坚持和贯彻以人民为中心的法治理念，牢牢把握保护人民群众个人信息权益的立法定位，聚焦个人信息保护领域的突出问题和人民群众的重大关切。

个人信息保护法共 8 章 74 条。在有关法律的基础上，该法进一步细化、完善个人信息保护应遵循的原则和个人信息处理规则，明确个人信息处理活动中的权利义务边界，健全个人信息保护工作体制机制。“个人信息保护法切实将广大人民群众网络空间合法权益维护好、保障好、发展好，使广大人民群众在数字经济发展中享受更多的获得感、幸福感、安全感。”**全国人大常委会法工委经济法室副主任杨合庆 20 日对个人信息保护法进行了权威解读。**

亮点一：确立个人信息保护原则

个人信息保护的原则是收集、使用个人信息的基本遵循，是构建个人信息保护具体规则的制度基础。

个人信息保护法借鉴国际经验并立足我国实际，确立了个人信息处理应遵循的原则，强调处理个人信息应当遵循合法、正当、必要和诚信原则，具有明确、合理的目的并与处理目的直接相关，采取对个人权益影响最小的方式，限于实现处理目的的最小范围，公开处理规

则，保证信息质量，采取安全保护措施等。“这些原则应当贯穿于个人信息处理的全过程、各环节。”杨合庆说。

亮点二：规范处理活动保障权益

个人信息保护法紧紧围绕规范个人信息处理活动、保障个人信息权益，构建了以“告知-同意”为核心的个人信息处理规则。

“‘告知-同意’是法律确立的个人信息保护核心规则，是保障个人对其个人信息处理知情权和决定权的重要手段。”杨合庆说。

个人信息保护法要求，处理个人信息应当在事先充分告知的前提下取得个人同意，个人信息处理的重要事项发生变更的应当重新向个人告知并取得同意。同时，针对现实生活中社会反映强烈的一揽子授权、强制同意等问题，个人信息保护法特别要求，个人信息处理者在处理敏感个人信息、向他人提供或公开个人信息、跨境转移个人信息等环节应取得个人的单独同意，明确个人信息处理者不得过度收集个人信息，不得以个人不同意为由拒绝提供产品或者服务，并赋予个人撤回同意的权利，在个人撤回同意后，个人信息处理者应当停止处理或及时删除其个人信息。

此外，考虑到经济社会生活的复杂性，个人信息处理的场景日益多样，个人信息保护法从维护公共利益和保障社会正常生产生活的角度，还对取得个人同意以外可以合法处理个人信息的特定情形作了规定。

此外，个人信息保护法还分别对共同处理、委托处理等实践中较为常见的处理情形作出有针对性规定。

亮点三：禁止“大数据杀熟”规范自动化决策

当前，越来越多的企业利用大数据分析、评估消费者的个人特征用于商业营销。有一些企业通过掌握消费者的经济状况、消费习惯、对价格的敏感程度等信息，对消费者在交易价格等方面实行歧视性的差别待遇，误导、欺诈消费者。其中，最典型的就是社会反映突出的“大数据杀熟”。

“‘大数据杀熟’行为违反了诚实信用原则，侵犯了消费者权益保护法规定的消费者享有公平交易条件的权利，应当在法律上予以禁止。”杨合庆说。

对此，个人信息保护法明确规定：个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。

亮点四：严格保护敏感个人信息

值得关注的是，个人信息保护法将生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息列为敏感个人信息。个人信息保护法要求，只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，方可处理敏感个人信息，同时应当事前进行影响评估，并向个人告知处理的必要性以及对个人权益的影响。

“这主要是考虑到此类信息一旦泄露或者被非法使用，极易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害，因此，对处理敏感个人信息的活动应当作出更加严格的限制。”杨合庆说。

值得关注的是，为保护未成年人的个人信息权益和身心健康，个人信息保护法特别将不满十四周岁未成年人的个人信息确定为敏感个人信息予以严格保护。同时，与未成年人保护法有关规定相衔接，要求处理不满十四周岁未成年人个人信息应当取得未成年人的父母或者其他监护人的同意，并应当对此制定专门的个人信息处理规则。

亮点五：规范国家机关处理活动

为履行维护国家安全、惩治犯罪、管理经济社会事务等职责，国家机关需要处理大量个人信息。保护个人信息权益、保障个人信息安全是国家机关应尽的义务和责任。但近年来，一些个人信息泄露事件也反映出有些国家机关存在个人信息保护意识不强、处理流程不规范、安全保护措施不到位等问题。

对此，个人信息保护法对国家机关处理个人信息的活动作出专门规定，特别强调国家机关处理个人信息的活动适用本法，并且处理个人信息应当依照法律、行政法规规定的权限和程序进行，不得超出履行法定职责所必需的范围和限度。

亮点六：赋予个人充分权利

个人信息保护法将个人在个人信息处理活动中的各项权利，包括知悉个人信息处理规则和处理事项、同意和撤回同意，以及个人信息的查询、复制、更正、删除等总结提升为知情权、决定权，明确个人有权限制个人信息的处理。

同时，为了适应互联网应用和服务多样化的实际，满足日益增长的跨平台转移个人信息的需求，个人信息保护法对个人信息可携带权作了原则规定，要求在符合国家网信部门规定条件的情形下，个人信息处理者应当为个人提供转移其个人信息的途径。

此外，个人信息保护法还对死者个人信息的保护作了专门规定，明确在尊重死者生前安排的前提下，其近亲属为自身合法、正当利益，可以对死者个人信息行使查阅、复制、更正、删除等权利。

亮点七：强化个人信息处理者义务

个人信息处理者是个人信息保护的第一责任人。据此，个人信息保护法强调，个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。

在此基础上，个人信息保护法设专章明确了个人信息处理者的合规管理和保障个人信息安全等义务，要求个人信息处理者按照规定制定内部管理制度和操作规程，采取相应的安全技术措施，指定负责人对其个人信息处理活动进行监督，定期对其个人信息活动进行合规审计，对处理敏感个人信息、利用个人进行自动化决策、对外提供或公开个人信息等高风险处理活动进行事前影响评估，履行个人信息泄露通知和补救义务等。

亮点八：赋予大型网络平台特别义务

互联网平台服务是数字经济区别于传统经济的显著特征。互联网平台为商品和服务的交易提供技术支持、交易场所、信息发布和交易撮合等服务。

“在个人信息处理方面，互联网平台为平台内经营者处理个人信息提供基础技术服务、设定基本处理规则，是个人信息保护的关键环节。”杨合庆指出，提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者对平台内的交易和个人信息处理活动具有强大的控制力和支配力，因此在个人信息保护方面应当承担更多的法律义务。

据此，个人信息保护法对这些大型互联网平台设定了特别的个人信息保护义务，包括：按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督；遵循公开、公平、公正的原则，制定平台规则；对严重违法处理个人信息的平台内产品或者服务提供者，停止提供服务；定期发布个人信息保护社会责任报告，接受社会监督。个人信息保护法的上述规定是为了提高大型互联网平台经营业务的透明度，完善平台治理，强化外部监督，形成全社会共同参与的个人信息保护机制。

亮点九：规范个人信息跨境流动

随着经济全球化、数字化的不断推进以及我国对外开放的不断扩大，个人信息的跨境流动日益频繁，但由于遥远的地理距离以及不同国家法律制度、保护水平之间的差异，个人信息跨境流动风险更加难以控制。

“个人信息保护法构建了一套清晰、系统的个人信息跨境流动规则，以满足保障个人信息权益和安全的客观要求，适应国际经贸往来的现实需要。”杨合庆介绍说，一是明确以向境内自然人提供产品或者服务为目的，或者分析、评估境内自然人的行为等，在我国境外处理境内自然人个人信息的活动适用本法，并要求符合上述情形的境外个人信息处理者在我国境内设立专门机构或者指定代表，负责个人信息保护相关事务；二是明确向境外提供个人信息的途径，包括通过国家网信部门组织的安全评估、经专业机构认证、订立标准合同、按照

我国缔结或参加的国际条约和协定等；三是要求个人信息处理者采取必要措施保障境外接收方的处理活动达到本法规定的保护标准；四是对跨境提供个人信息的“告知-同意”作出更严格的要求，切实保障个人的知情权、决定权等权利；五是为维护国家主权、安全和发展利益，对跨境提供个人信息的安全评估、向境外司法或执法机构提供个人信息、限制跨境提供个人信息的措施、对外国歧视性措施的反制等作了规定。

亮点十：健全个人信息保护工作机制

个人信息保护涉及的领域广，相关制度措施的落实有赖于完善的监管执法机制。

根据个人信息保护工作实际，个人信息保护法明确，国家网信部门和国务院有关部门在各自职责范围内负责个人信息保护和监督管理工作，同时，对个人信息保护和监管职责作出规定，包括开展个人信息宣传教育、指导监督个人信息保护工作、接受处理相关投诉举报、组织对应用程序等进行测评、调查处理违法个人信息处理活动等。

此外，为了加强个人信息保护监管执法的协同配合，个人信息保护法还进一步明确了国家网信部门在个人信息保护监管方面的统筹协调作用，并对其统筹协调职责作出具体规定。

（来源：法制日报）

➢ 加强关键信息基础设施安全保护的法治基石

新世纪以来，以互联网为代表的信息技术革命在全球迅速普及和应用，推动经济社会的数字化转型并带来了生产力新的解放和飞跃。关键信息基础设施的安全保护已经成为各国推进数字经济发展、参与国际竞争的重要保障。习近平总书记的重要指示为我们建设国家关键信息基础设施安全保障体系指明了方向。当今世界正经历百年未有之大变局，国际环境日趋复杂，不稳定性不确定性明显增强。关键信息基础设施安全事关国家网络安全和数据安全，日益成为国家网络空间安全能力建设的核心和关键。

近日，国务院正式公布了《关键信息基础设施安全保护条例》（以下简称《条例》）。该《条例》是我国针对关键信息基础设施安全保护的专门性行政法规，也是指导国家网络安全保障工作的基础性行政法规。认真学习领会《条例》内容，对于推动关键信息基础设施安全保障能力建设，维护国家网络空间主权和安全利益具有深刻意义。

一、制定《关键信息基础设施安全保护条例》立法背景认识

关键信息基础设施在国家经济和社会服务中承担着重要角色并发挥着关键作用。随着我

国国民经济和社会信息化的全面推进，传统的社会活动不断向网络空间延伸扩展，经济与国家安全高度依赖于关键信息基础设施。完善关键信息基础设施保护法律体系，全面提升关键信息基础设施安全保护意识、保障能力和水平，已经成为网络安全博弈的制胜关键。

党的十八大以来，以习近平同志为核心的党中央高度重视关键信息基础设施安全保护工作，就加强关键信息基础设施安全保护工作作出了一系列重大决策和部署。在中央网络安全和信息化领导小组第一次会议上，习近平总书记指出，要完善关键信息基础设施保护等法律法规。在 2016 年的网络安全和信息化工作座谈会上，习近平总书记明确要求“加快构建关键信息基础设施安全保障体系”。2021 年我国发布的《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》明确强调要“建立健全关键信息基础设施保护体系，提升安全防护和维护政治安全能力”。作为“十四五”开局之年发布的一项重要法规，《条例》是推动我国网络安全法治化工作的又一项重要举措和成果，对建立健全我国关键信息基础设施安全保护体系具有里程碑式的意义。《条例》从突出重点保护、坚持问题导向、与已有相关法律法规有效衔接三方面出发，科学总结网络安全工作实践经验，并上升为法规制度，为关键信息基础设施安全保护工作提供法治保障。

二、《条例》重点内容理解

从内容上看，《条例》坚持总体国家安全观和习近平总书记关于网络强国的重要思想，坚持安全发展、改革创新、问题导向的指导方针，坚持综合协调、分工负责、依法保护，充分发挥行政法规的引领和推动作用，加快推进关键信息基础设施安全保障体系建设。具体来说，《条例》主要内容有以下几个亮点：

一是明晰了关键信息基础设施的定义，并按照抓重点、保关键的思路，围绕关键、信息、基础这三个要素科学界定了关键信息基础设施的范围。《条例》站在总体国家安全观的视角，对关键信息基础设施范围的明确界定，有利于更好地推动国家网络空间安全核心能力建设，筑牢国家网络空间安全的屏障。

二是明确了保护工作部门职责，在充分考虑重点行业、领域业务及网络安全需求的特殊性、专业性的前提下，将行业领域主管监管部门明确为关键信息基础设施安全保护部门，组织领导和监督管理本行业、本领域关键信息基础设施安全保护工作。

三是强化了运营者安全管理，特别强调建立“一把手负责制”，明确了运营者主要负责人负总责，切实保障人财物投入，为安全保护工作的物质基础提供了法律保障。

四是规定了国家保障和促进措施。《条例》明确了建立网络安全信息共享机制、完善监测预警和应急体系、组织开展检查检测、能源和通信服务优先保障、加强安全保卫和防范打击违法犯罪、出台相应标准指导规范等 6 个方面的保障措施。为体现国家重点支持，《条例》从人才培养、财政金融、技术创新、产业发展、军民融合、表彰奖励、宣传教育等 7 个方面提出了促进措施。

五是确立了监督管理体制。《条例》规定，在国家网信部门统筹协调下，国务院公安部门负责指导监督关键信息基础设施安全保护工作；国务院电信主管部门和其他有关部门依照本条例和有关法律、行政法规的规定，在各自职责范围内负责安全保护和监督管理工作；省级人民政府有关部门依据各自职责对关键信息基础设施实施安全保护和监督管理。

三、关键信息基础设施安全保护工作重点任务的思考

在网络安全威胁和风险日益突出，关键信息基础设施面临的安全形势日趋严峻的大背景下，《条例》的出台正当其时，也时不我待。《条例》正式实施后，我国关键信息基础设施安全保护工作将进入新的发展阶段，关于未来相关工作重点任务主要有以下几方面的思考：

（一）关键信息基础设施是国家网络安全保障工作的核心和基石，需要国家总体部署、统筹协调。

关键信息基础设施承载或支撑着重要行业和领域关键业务，并成为各行各业运行体系所依赖的关键节点，一旦遭到破坏，通过关联行业、领域逐渐传递，会给国民经济和国家安全造成连锁连片影响的严重后果。作为经济社会运行的神经中枢，关键信息基础设施日益发挥着基础性、全局性、支撑性作用，“牵一发而动全身”。因此，提升我国网络安全保障能力，筑牢国家网络安全屏障，维护国家网络空间主权和国家安全，就要切实抓住关键信息基础设施安全这个“牛鼻子”。

作为国家网络安全保障的核心及全局性工作，关键信息基础设施安全保护必须要坚持总体部署。从这个意义上来说，在中央网络安全和信息化委员会领导下，国家网信部门应发挥好统筹协调职能，不断强化关键信息基础设施安全保护工作的顶层设计、总体布局、统筹协调、整体推进。国务院公安部门加强对关键信息基础设施安全保护工作的指导监督。国务院电信主管部门和其他有关部门应根据《条例》规定的职责实施安全保护和监督管理。

（二）持续性的能力评估是完善关键信息基础设施安全保护工作的引导和方向。

通过总结我国关键信息基础设施保护实践经验以及相关法律政策的保护要求，在“十四五”时期，提出适合于我国的关键信息基础设施安全保护能力水平评估体系具有重要的现实意义。安全能力评估是关键信息基础设施安全保护的重要环节，其结果可以直接反映关键信息基础设施的安全保护状况，发现存在的薄弱点，并为关键信息基础设施安全整改和后期安全规划制定提供依据。从长远上看，持续性能力评估是为关键信息基础设施的建设运维管理保障提供了方向，能够起到以评促建、以评促管、以评促改的效果。

（三）做好关键信息基础设施安全保护工作要切实发挥我国制度优势，集聚社会各界力量。

一是要充分发挥我国集中力量办大事的体制优势，进一步加强政企合作、军地协同，发挥政策优势，要由自我保护向国家、行业、运营者共同保护转变，形成工作合力，共同推动关键信息基础设施安全保护工作，应对风险挑战。二是要继续做大做强我国网络安全产业，培育一批自主核心技术突出、经济效益优势明显、生态引领能力显著的领航型品牌企业，以及保障具有技术特色、成长性好的中小企业健康成长，依托其技术、产品、人力和服务优势，整合共享资源，推进安全保护的集约化、专业化、常态化，更好地为关键信息基础设施安全保障提供支撑。三是要发挥行业组织的桥梁纽带作用，积极对接关键信息基础设施运营者与网络安全技术、服务提供者供需双方的实际需求，有力支撑关键信息基础设施安全保护技术创新和产业发展。四是要持续做好关键信息基础设施安全保护相关政策宣贯工作，建议将关键信息基础设施安全保护的相关法律法规学习纳入领导干部和相关企业负责同志的网络安全意识培训之中，将贯彻落实情况逐步纳入各级关键信息基础设施安全保护责任部门和机构的考核之中，并通过“国家网络安全宣传周”等常态化网络安全宣传教育活动，动员全社会共同参与，切实提升全社会关键信息基础设施安全保护意识，形成国家网络安全的强大凝聚力和向心力。

《条例》为我国营造开放、安全、健康的数字生态，巩固国家网络安全保障基础，强化数字资源安全保护能力提供了坚强的法治后盾，也为关键信息基础设施安全保护工作提供了

科学化、系统化、精细化的工作指引。展望“十四五”时期，随着《条例》的实施，我国网络安全工作必将乘势而上，向着实现网络强国战略目标不断奋勇前进。（来源：司法部）

➢ 大数据时代的信息安全

《中华人民共和国数据安全法》即将于 9 月 1 日起生效施行。近日，工信部委托中国互联网协会召开头部平台座谈会，召集国内 12 家知名企业参加，要求强化平台数据管理责任，明确数据安全责任人，并加强重要数据安全评估和出境管理。

当前，大数据正在成为信息时代的核心战略资源，对国家治理能力、经济运行机制、社会生活方式产生深刻影响。与此同时，各项技术应用背后的数据安全风险也日益凸显。近年来，有关数据泄露、数据窃听、数据滥用等安全事件屡见不鲜，保护数据资产已引起各国高度重视。在我国数字经济进入快车道的时代背景下，如何开展数据安全治理，提升全社会的“安全感”，已成为普遍关注的问题。

数据是 21 世纪的石油和钻石

所谓数据，“是指对客观事件进行记录并可以鉴别的符号，是对客观事物的性质、状态以及相互关系等进行记载的物理符号或这些物理符号的组合。它是可识别的、抽象的符号。”

当前，我们已经进入到了一个大数据时代。大数据解决了以往必须由局部去推测整体的困难。就像我们在大海航行时发现了冰山一角，以往必须借助于某种“算法”去推测整个冰山的大小，现在则能较为轻松地获得冰山的“大数据”，整个冰山一览无余地呈现在面前，使我们能够趋利避害，在大海上安全航行。可以说，大数据作为“人类一种新型的、功能强

大的好工具”，使我们能够迅速把握事物的整体、相互关系和发展趋势，从而做出更加准确的预判、更加科学的决策、更加精准的行动。

如今，数据作为数字经济时代最核心、最具价值的生产要素，正深刻地改变着人类社会的生产和生活方式。人工智能、云计算、区块链、产业互联网、泛在感知等新技术、新模式、新应用无一不是以海量数据为基础。年度账单、运动轨迹……互联网应用平台对用户使用情况的“个人总结”成了人们津津乐道的话题。一张张有趣的“用户画像”背后，是大数据应用越来越深入寻常百姓家的时代烙印。

特别是受新冠肺炎疫情的影响，以数据为核心的数字技术逐步成为经济发展的新驱动力，也深刻地改变人们的日常生活。实施疫情地图使我们对全国的疫情防控形势一切尽在“掌”握，社区门禁的人脸识别功能使我们可以“刷脸”通关，“健康宝”成为了我们的随身证件，“行程码”也成了“旅行必备”……大数据在疫情期间的应用发展，不仅为疫情监测、防控救治、资源调配等提供了有效指引，也给全社会上了一堂生动的数据科普课，彰显了大数据作为国家基础性战略资源的重要意义。

与此同时，持续增加的数据资源及其存储和处理技术的变化，也逐步成为一种潜在增长、可持续累积的社会资源。据相关机构预测，2025 年全球数据量将高达 175ZB。其中，中国数据量增速最为迅猛，预计 2025 年将增至 48.6ZB，成为全球最大的数据圈。

为了进一步整合数据资源，加快建设数据强国，早在 2015 年，国务院便已经出台了《促进大数据发展行动纲要》。其中，明确指出“坚持创新驱动发展，加快大数据部署，深化大数据应用，已成为稳增长、促改革、调结构、惠民生和推动政府治理能力现代化的内在需要和必然选择”，强调要“推动大数据发展和应用，在未来 5 至 10 年打造精准治理、多方协作的社会治理新模式，建立运行平稳、安全高效的经济运行新机制，构建以人为本、惠及全民的民生服务新体系，开启大众创业、万众创新的创新驱动新格局，培育高端智能、新兴繁荣的产业发展新生态”。

数据安全是数字经济健康发展的基础

几年前在广州举行的世界安防博览会上，几乎每一个厂商都会极力向观众介绍，我的人脸识别技术有多厉害，从性别、年龄、穿着等信息都可以高度还原。而今年 7 月 29 日到 31 日举行的安博会，几乎没有一家厂商再浓墨重彩展示自身人脸识别技术中的数据采集，取而代之的则是更偏向于后端的数据治理。在《数据安全法》即将实施之际，这场安博会有了新意。

根据《数据安全法》和其他一些相关法规的要求，商家必须对所收集的数据负安全责任。

掌握的数据越多，担负的责任就越大。这一规则，对人脸识别单位来说同样适用。我们都知道，单条的身份信息、轨迹信息、视频信息看起来都没有特别的价值，但是如果把这些信息拼接起来，再通过大数据分析，就可以得到很多重要的信息。

截至去年底，中国网民已经达 9.89 亿。网购、网约车、网上银行等互联网服务已经全方位介入现实生活。人们为了获取便利高效的服务，已习惯录入自己的姓名、电话、住址、银行卡号等隐私信息。从某种意义上讲，在大数据技术的背景下，绝大部分数据来自于用户“自愿”提供。

同时，人们在各种社交媒体上发布的动态和信息会在不经意间暴露自身的敏感信息，这也使个人信息更容易“公开”。根据最新研究显示，只要有一个人的年龄、性别和邮编，就能从公开的数据中搜索到这个人 87%的个人信息。

随着定位技术的高速发展以及物联网、大数据和人工智能等技术的不断发展与应用，无论是微博、微信、QQ 等网络社交应用，还是涉及人们衣食住行的其他相关应用，都存在着个人数据外泄的可能。

数据的使用与搜集都具有高度隐蔽性，但结合强大的数据分析能力，便让众多用户无形中成为“被监控”的对象。于是“天知地知、你知我知”的数据变得“人尽皆知”。数据使用便利的同时，让渡的是隐患重重的消费者隐私安全，甚至是国家安全。

以我们经常坐的网约车为例，一些网约车企业在长期的业务开展中，积累了海量的出行数据与地图信息。此外，汽车在使用过程中联动的摄像头、传感器等，都涉及众多数据安全问题，消费者的个人隐私、企业的商业机密乃至国家安全，都有可能受到严重威胁。

“美国国家安全局以及网络巨头的关系正是计算能力和海量数据的结合，因此全球大部分数据都掌握在他们手中。”全国信息安全标准化技术委员会委员谈剑峰介绍，大量的数据在网上是没有保护的。

据统计，2020 年全球数据泄露超过去 15 年总和。其中，政务、医疗及生物识别信息等高价值特殊敏感数据泄露风险加剧，云、端等数据安全威胁居高不下，数据交易黑色地下产业链活动猖獗。

今年 5 月，由国家工业信息安全发展研究中心和华为公司联合发布的《数据安全白皮书》指出，数据安全已经上升到国家主权的高度，是国家竞争力的直接体现，是数字经济健康发展的基础。这就要求我们必须解决数据安全领域的突出问题，有效提升数据安全治理能力。

既要数据安全 也要数据畅通

当前形势下，我们要如何保护数据安全？

数据保护是在进行数字化转型的大背景下，在数据流动和使用状态中的数据保护，不同于以前防火墙式的静态保护，数据安全治理更倾向于动态保护。

数据安全治理能力建设需要从决策到技术、从制度到工具、从组织架构到安全技术的通盘考虑，既要注重“硬实力”的锻造，也要聚焦“软实力”的提升。

一方面，在技术设施领域，要持续提升数据安全的产业基础能力，构筑技术领先、自主创新的数据基座，确保数据基础设施安全可靠。同时，不断强化数据安全领域关键基础技术的研究与应用，在芯片、操作系统、人工智能等方面，加强密码技术基础研究，推进密码技术的成果转化，确保基础软件自主可控。

另一方面，要健全数据安全法律法规，不断强化法律法规在数据安全主权方面的支撑保障作用。据不完全统计，近 5 年来我国国家、地方省市以及各行业监管部门关于数据安全、网络安全已颁布 50 多部相关法律法规。《数据安全法》的出台，也预示着我国数据开发与应用将全面进入法治化轨道。

比如，《数据安全法》第 32 条规定：“任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。法律、行政法规对收集、使用数据的目的、范围有规定的，应当在法律、行政法规规定的目的和范围内收集、使用数据。”互联网企业收集数据应符合此条规定，否则将面临法律风险。

此外，《数据安全法》第 36 条规定：“非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。”

新法案扩大了向境外提供数据的监管适用情形，即只要中国境外的司法或者执法机构要求提供存储于中国境内的数据，均适用本条的规定，有助于更好地封堵境外机构的“长臂管辖”。

《数据安全法》既要数据安全，也保护数据的交易和流通，鼓励使用大数据创新，鼓励使用数据驱动业务。打个比喻，一栋大楼的门窗锁就是它的硬性保护措施，而在此之后，大楼可能会装监控、摄像头、X 光机等安检设备，这就是数据安全。防盗门是直接把人拒之门外的，但安检则是检查合格后可以进去。所以，数据安全是更高层面的安全措施，它不会阻碍数据的流动。

值得注意的是，从已经出台的《网络安全法》到即将施行的《数据安全法》，再到酝酿中的《个人信息保护法》，一个共通的原则就是对数据的使用收集要克制，明确哪些数据是必须要收集的，如果不能收集，就要有相应的制度规范。

在希腊神话中，伊卡洛斯与父亲代达罗斯使用蜡和羽毛制造的羽翼逃离克里特岛，由于过分相信自己的飞行技术，所以飞得太高，结果双翼上的蜡在太阳照射下逐渐融化，导致羽翼脱落，最终葬身大海。大数据是把“双刃剑”，大数据技术如同“蜡和羽毛”制作的翅膀，它可以帮助我们飞得更高，但是如果我们不对其规范，便有葬身大海的风险。信息安全意识和保护能力的提升是防止数据泄露的关键。我们在享受数据红利的同时，数据安全保护这根弦须臾不能放松。（来源：中央纪委国家监委网站）

➢ 让手机应用程序清爽起来

打开常用的手机应用程序(APP)，开屏广告有了关闭按钮；关闭开屏广告后，界面变得干净清朗，开启速度也快了不少……近期，针对用户反映强烈、投诉较多的手机 APP 诱导用户点击跳转、弹窗广告难以关闭等违规行为，工信部进行了集中整治，取得阶段性成果。

近年来，随着移动互联网的迅速发展，各类手机 APP 逐渐成为人们日常生活的“必需品”。但与此同时，一些手机 APP 广告存在“弹窗信息标识近于无形、关闭按钮小如蝼蚁、页面伪装瞒天过海、诱导点击暗度陈仓”等问题，令人不胜其扰。这既降低了用户体验，也潜藏着侵害用户权益的风险。无论是从保护用户合法权益和隐私安全来说，还是从维护网络服务秩序而言，都有必要加大治理力度。也正因此，工信部的这一次集中整治，赢得多方叫好。

手机 APP 接入广告本身并无不可，关键在于相关操作要符合法律规定。广告法第四十

四条明确规定：“利用互联网发布、发送广告，不得影响用户正常使用网络。在互联网页面以弹出等形式发布的广告，应当显著标明关闭标志，确保一键关闭。”互联网广告管理暂行办法第八条也规定：“不得以欺骗方式诱使用户点击广告内容。”从去年 3 月，国家市场监督管理总局等 11 部门联合印发通知，强调坚决遏制移动 APP、自媒体账号等虚假违法广告多发、易发态势；到去年 10 月，国家网信办针对手机 APP 弹窗广告乱象，出台首批专项整治名单；再到工信部这次开展的手机 APP 专项整治行动，近年来相关部门付出不少努力，治理成效显著。数据显示，今年第二季度，手机 APP 开屏弹窗信息用户投诉举报数量环比下降 50%，误导用户点击跳转第三方页面问题同比下降 80%。

成效值得肯定，治理还需持之以恒。移动互联网时代，注意力是稀缺资源，植入广告、流量变现成为许多应用程序盈利的手段。在利益驱使下，有的商家不免心存侥幸、铤而走险。这也是为何一些手机 APP 广告关不掉、退不出的一个重要原因。同时，手机 APP 种类繁多，不同类别 APP 从事广告经营活动的方式和发布主体不尽相同，也给治理增加了难度。治理手机 APP 广告，是一项长期工作，还需久久为功。一方面，应加大制度供给，严格规范手机 APP 广告，比如可以引入“黑名单”制度等，提升违法成本。另一方面，也应善用技术，破解难题。比如，运用好大数据、人工智能等技术手段，精准识别和监测手机 APP 平台的广告投放，强化监管的针对性。

让手机 APP 清爽起来，不仅需要监管机构发挥作用，也需要运营平台把好广告的“内容关”。用户选择一款手机 APP，既有方便的考虑，更有舒心的衡量。因此，对于手机 APP 运营商而言，要有用户意识。只有赢得口碑，才能赢得市场。把用户权益、使用体验和社会责任扛在肩上、放在心里，这是企业行稳致远的必然选择，也是手机 APP 赢得用户的关键所在。（来源：人民日报）

四、政府之声

➢ 《关键信息基础设施安全保护条例》发布 2021 年 9 月 1 日起施行

2021 年 7 月 30 日，国务院总理李克强签署第 745 号国务院令，公布《关键信息基础设施安全保护条例》(以下简称《条例》)，自 2021 年 9 月 1 日起施行。日前，司法部、网信办、工业和信息化部、公安部负责人就《条例》有关问题回答了记者提问。

问：请简要介绍一下《条例》出台的背景?

答：党中央、国务院高度重视关键信息基础设施安全保护工作。关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重。保障关键信息基础设施安全，对于维护国家网络空间主权和国家安全、保障经济社会健康发展、维护公共利益和公民合法权益具有重大意义。当前，关键信息基础设施面临的网络安全形势日趋严峻，网络攻击威胁上升，事故隐患易发多发，安全保护工作还存在法规制度不完善、工作基础薄弱、资源力量分散、技术产业支撑不足等突出问题，亟待建立专门制度，明确各方责任，加快提升关键信息基础设施安全保护能力。2017 年施行的《中华人民共和国网络安全法》规定，关键信息基础设施的具体范围和安全保护办法由国务院制定。出台《条例》旨在落实《中华人民共和国网络安全法》有关要求，将为我国深入开展关键信息基础设施安全保护工作提供有力法治保障。

问：制定《条例》的总体思路是什么?

答：在总体思路上主要把握了以下三点：一是坚持问题导向。针对关键信息基础设施安全保护工作实践中的突出问题，细化《中华人民共和国网络安全法》有关规定，将实践证明成熟有效的做法上升为法律制度，为保护工作提供法治保障。二是压实责任。坚持综合协调、

分工负责、依法保护，强化和落实关键信息基础设施运营者主体责任，充分发挥政府及社会各方面的作用，共同保护关键信息基础设施安全。三是做好与相关法律、行政法规的衔接。在《中华人民共和国网络安全法》确立的制度框架下，细化相关制度措施，同时处理好与相关法律、行政法规的关系。

问：开展关键信息基础设施安全保护工作，各部门的职责分工是什么？

答：《条例》第三条规定在国家网信部门统筹协调下，国务院公安部门负责指导监督关键信息基础设施安全保护工作;国务院电信主管部门和其他有关部门依照本条例和有关法律、行政法规的规定，在各自职责范围内负责关键信息基础设施安全保护和监督管理工作。省级人民政府有关部门依据各自职责对关键信息基础设施实施安全保护和监督管理。

问：关键信息基础设施如何认定？

答：《条例》从我国国情出发，借鉴国外通行做法，明确了关键信息基础设施的定义和认定程序。一是明确关键信息基础设施的定义。二是明确关键信息基础设施所在行业和领域的主管部门、监督管理部门是负责关键信息基础设施安全保护工作的部门。三是明确由保护工作部门结合本行业、本领域实际，制定关键信息基础设施认定规则，并组织认定本行业、本领域的关键信息基础设施。四是规定关键信息基础设施发生较大变化，可能影响其认定结果时，运营者应当及时报告保护工作部门，由保护工作部门重新认定。

问：《条例》对保护工作部门职责作了哪些规定？

答：依据《中华人民共和国网络安全法》有关规定，按照“谁主管谁负责”的原则，《条例》明确了保护工作部门对本行业、本领域关键信息基础设施的安全保护责任：一是制定关键信息基础设施安全规划，明确保护目标、基本要求、工作任务、具体措施。二是建立健全网络安全监测预警制度，及时掌握关键信息基础设施运行状况、安全态势，预警通报网络安全威胁和隐患，指导做好安全防范工作。三是建立健全网络安全事件应急预案，定期组织应急演练。四是指导运营者做好网络安全事件应对处置，并根据需要组织提供技术支持与协助。五是定期组织开展网络安全检查检测，指导监督运营者及时整改安全隐患、完善安全措施。

问：为强化和落实关键信息基础设施运营者主体责任，《条例》主要作了哪些规定？

答：《条例》在总则部分对运营者责任作了原则规定，要求运营者依照本条例和有关法律、行政法规的规定以及国家标准的强制性要求，在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。

《条例》还设专章细化了有关义务要求，主要包括：一是建立健全网络安全保护制度和

责任制，实行“一把手负责制”，明确运营者主要负责人负总责，保障人财物投入。二是设置专门安全管理机构，履行安全保护职责，参与本单位与网络安全和信息化有关的决策，并对机构负责人和关键岗位人员进行安全背景审查。三是对关键信息基础设施每年进行网络安全检测和风险评估，及时整改问题并按要求向保护工作部门报送情况。四是关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，按规定向保护工作部门、公安机关报告。五是优先采购安全可信的网络产品和服务，并与提供者签订安全保密协议;可能影响国家安全的，应当按规定通过安全审查。

问：对于关键信息基础设施安全保护工作，《条例》明确了哪些保障和促进措施?

答：保障关键信息基础设施安全，需要统筹资源和力量，全方位实施保护。《条例》在保障方面，一是明确建立网络安全信息共享机制，并规定工作中获取的信息只能用于维护网络安全，不得泄露、出售或者非法向他人提供。二是对国家有关部门开展安全检查作出规定，要求避免不必要的检查和交叉重复检查，检查不得收费，不得要求被检查单位购买指定产品和服务;同时规定任何个人和组织未经授权不得对关键信息基础设施进行探测测试等活动。三是规定国家网信部门和国务院电信主管部门、公安部门等根据保护工作部门需要，提供技术支持和协助。四是明确国家对能源、电信等关键信息基础设施安全运行实施优先保障。五是规定公安机关、国家安全机关依据各自职责依法加强关键信息基础设施安全保卫，防范打击针对和利用关键信息基础设施实施的违法犯罪活动。六是明确国家出台安全标准，指导规范关键信息基础设施安全保护工作。《条例》在支持促进方面，从人才培养、技术创新和产业发展、网络安全服务机构建设与管理、军民融合、表彰奖励等方面作了相应规定。

问：对实施危害关键信息基础设施安全活动的个人和组织，或未经授权或批准，对关键信息基础设施实施漏洞探测、渗透性测试等活动的个人和组织，《条例》作了哪些规范?

答：实践中，一些个人和组织擅自对关键信息基础设施实施漏洞探测、渗透性测试等活动，影响关键信息基础设施安全。《条例》一是明确任何个人和组织不得实施非法侵入、干扰、破坏关键信息基础设施的活动，不得危害关键信息基础设施安全。二是规定未经国家网信部门、国务院公安部门批准或者保护工作部门、运营者授权，任何个人和组织不得对关键信息基础设施实施漏洞探测、渗透性测试等可能影响或者危害关键信息基础设施安全的活动。对基础电信网络实施漏洞探测、渗透性测试等活动，应当事先向国务院电信主管部门报告。三是在法律责任章节中专门规定了相应罚则。

问：关键信息基础设施中的重要数据出境如何进行?

答：《中华人民共和国数据安全法》已由第十三届全国人民代表大会常务委员会第二十

九次会议于 2021 年 6 月 10 日通过，将于 9 月 1 日起实施。其中，第三十一条规定，关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定。《中华人民共和国网络安全法》第三十七条规定，关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估;法律、行政法规另有规定的，依照其规定。（来源：国务院）

- **中华人民共和国国务院令第 745 号《关键信息基础设施安全保护条例》**
- **全文：**http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm

➢ 《中华人民共和国个人信息保护法》2021 年 11 月 1 日施行

2021 年 8 月 20 日，《中华人民共和国个人信息保护法》由十三届全国人大常委会第三十次会议正式通过，这翻开了我国个人信息立法保护的历史新篇章，也是全球个人信息法治发展的重大里程碑。

个人信息保护法全文以总计 8 章 74 条的篇幅，在总则、个人信息处理规则、个人信息跨境提供的规则、个人在个人信息处理活动中的权利、个人信息处理者的义务、履行个人信息保护职责的部门、法律责任以及附则等多个层面设计和建构个人信息保护的立法框架，在

条文内容上反映了立法者吸收接轨国际立法、探索开创中国路径的制度努力，特别是在规范设计上呈现了众多亮点。（来源：中国人大网）

- **《中华人民共和国个人信息保护法》全文：**
- http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

➢ 五部门联合发布《汽车数据安全管理若干规定（试行）》

2021 年 8 月 16 日，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、交通运输部联合发布《汽车数据安全管理若干规定（试行）》（以下简称《规定》）。国家互联网信息办公室有关负责人就《规定》相关问题回答了记者提问。

问：请简要介绍《规定》出台的背景？

答：出台《规定》主要基于以下两方面的考虑：一是防范化解汽车数据安全风险的实践需要。汽车产业涉及国家经济、装备制造、金融、交通运输、生产生活等诸多领域，汽车数据处理能力日益增强、汽车数据规模庞大，同时暴露出的汽车数据安全问题和风险隐患也日益突出。比如，汽车数据处理者超越实际需要，过度收集重要数据；未经用户同意，违规处理个人信息，特别是敏感个人信息；未经安全评估，违规出境重要数据等。因此，亟需加强汽车数据安全管理，防范化解上述安全问题和风险隐患。二是保障汽车数据依法合理有效利用的客观需要。《网络安全法》、《数据安全法》对数据安全、个人信息保护作了基本规定。在汽车数据安全管理领域出台有针对性的规章制度，明确汽车数据处理者的责任和义务，规

范汽车数据处理活动，有利于促进汽车数据依法合理有效利用和汽车行业健康有序发展。

此外，还要说明的是，《规定》定位于若干规范要求，聚焦汽车领域个人信息和重要数据的安全风险，就若干重点问题作出规定。

问：《规定》中所称汽车数据和汽车数据处理活动是指什么？

答：《规定》中所称汽车数据，是指汽车设计、生产、销售、使用、运维等过程中的涉及个人信息数据和重要数据；所称汽车数据处理，包括汽车数据的收集、存储、使用、加工、传输、提供、公开等，涉及汽车数据处理的全生命周期。《规定》还进一步明确了汽车数据中的个人信息、敏感个人信息、重要数据以及汽车数据处理者的含义和类型。

问：《规定》明确了汽车数据处理者开展汽车数据处理活动应当符合哪些一般要求？

答：《规定》明确了汽车数据处理者开展汽车数据处理活动的一般要求。主要包括：一是处理汽车数据应当合法、正当、具体、明确，与汽车的设计、生产、销售、使用、运维等直接相关。二是利用互联网等信息网络开展汽车数据处理活动，应当落实网络安全等级保护等制度，加强汽车数据保护，依法履行数据安全义务。三是应当建立投诉举报渠道，设置便捷的投诉举报入口，及时处理用户投诉举报。

问：《规定》倡导汽车数据处理者在开展汽车数据处理活动中坚持哪些原则？

答：《规定》制定过程中，坚持安全和发展并重，倡导汽车数据处理者在开展汽车数据处理活动中坚持“车内处理”、“默认不收集”、“精度范围适用”、“脱敏处理”等原则，减少对汽车数据的无序收集和违规滥用，鼓励汽车数据依法合理有效利用，促进汽车行业健康有序发展。

问：为了使汽车数据处理者更好地履行个人信息保护责任，《规定》明确了哪些具体要求？

答：《规定》明确了处理个人信息、敏感个人信息的具体要求。针对个人信息，一是告知义务，汽车数据处理者处理个人信息应当告知处理个人信息种类、收集情境、停止收集方式途径等相关信息。二是征得同意义务，汽车数据处理者处理个人信息应当取得个人同意或者符合法律、行政法规规定的其他情形。三是匿名化要求，因保证行车安全需要，无法征得个人同意采集到个人信息且向车外提供的，应当进行匿名化处理。针对敏感个人信息，在履行告知、征得个人单独同意等义务基础上，汽车数据处理者处理敏感个人信息还应当满足限定处理目的、提示收集状态、为个人终止收集提供便利等具体要求。针对个人生物识别特征信息，明确汽车数据处理者具有增强行车安全的目的和充分的必要性方可收集。

问：为了规范重要数据处理活动，《规定》明确了哪些具体要求？

答：《规定》明确了处理重要数据的具体制度。一是风险评估报告制度，汽车数据处理者开展重要数据处理活动，应当按照规定开展风险评估，并向省、自治区、直辖市网信部门和有关部门报送风险评估报告。二是出境安全评估制度，重要数据应当依法在境内存储，因业务需要确需向境外提供的，应当通过国家网信部门会同国务院有关部门组织的安全评估。三是抽查核验制度，国家网信部门会同国务院有关部门以抽查等方式核验汽车数据出境评估有关事项，汽车数据处理者应当予以配合。四是年度报告制度，汽车数据处理者应当在每年十二月十五日前向省、自治区、直辖市网信和有关部门报送年度汽车数据安全管理情况。五是年度补充报告制度，向境外提供重要数据的汽车数据处理者应当补充报告相关情况。

问：关于汽车数据安全监督管理和保障，《规定》还明确了哪些具体措施？

答：除了上述报告、评估、抽查核验等监督管理措施以外，《规定》还明确国家网信部门和国务院发展改革、工业和信息化、公安、交通运输等有关部门依据职责，可根据处理数据情况对汽车数据处理者进行数据安全评估；明确国家加强智能（网联）汽车网络平台建设，开展智能（网联）汽车入网运行和安全保障服务等，协同汽车数据处理者加强智能（网联）汽车网络和汽车数据安全防护。

问：违反《规定》如何追究法律责任？

答：《规定》明确汽车数据处理者违反本规定的，由省级以上网信、工业和信息化、公安、交通运输等有关部门依照《网络安全法》、《数据安全法》等法律、行政法规的规定进行处罚；构成犯罪的，依法追究刑事责任。（来源：中国网信网）

- **《汽车数据安全管理若干规定（试行）》**
- **全文：**http://www.cac.gov.cn/2021-08/20/c_1631049984897667.htm

➢ 最高检下发通知 明确个人信息保护公益诉讼办案重点

2021 年 8 月 20 日，第十三届全国人民代表大会常务委员会第三十次会议通过的《中华人民共和国个人信息保护法》，将于 2021 年 11 月 1 日起正式实施。该法专门设立公益诉讼条款，明确将个人信息保护纳入检察公益诉讼法定领域。

2021 年 8 月 21 日，最高人民检察院下发**《关于贯彻执行个人信息保护法推进个人信息保护公益诉讼检察工作的通知》**(下称《通知》)，规范相关公益诉讼案件办理，切实履行好公益诉讼检察的法定职责。

个人信息保护法第七十条明确规定：“个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。”

《通知》指出，加强个人信息公益保护，是贯彻落实习近平法治思想，推进国家治理，强化法律监督的必然要求，要深刻领会个人信息保护法设置公益诉讼条款的重要意义，进一步增强检察履职的责任感和紧迫感，切实加大办案力度，推动公益诉讼条款落地落实。

《通知》明确，根据个人信息保护法有关规定，各级检察机关在履行公益诉讼检察职责时应当突出重点、从严把握以下方面：生物识别、宗教信仰、特殊身份、医疗健康、金融账号、行踪轨迹等敏感个人信息应当严格保护;儿童、妇女、残疾人、老年人、军人等特殊群体的个人信息需要特别保护;教育、医疗、就业、养老、消费等重点领域处理的个人信息，以及处理 100 万人以上的大规模个人信息应当重点保护;对因时间、空间等联结形成的特定对象的个人信息加强精准保护。

《通知》强调，要构建完善个人信息保护办案流程机制，充分发挥检察一体化办案优势。各级检察机关要用足用好《人民检察院公益诉讼办案规则》中关于调查核实权的有关规定，充分运用科技手段，借助公安、工信等部门的专业技术力量，完善检察技术人员参加公益诉讼办案机制。个人信息保护法正式施行后，最高检、省级检察院要加大自办案件和对下指导力度，采取上级院交办、提办、督办、领办等方式，以检察一体化应对个人信息公益损害网络化。

《通知》要求，要延伸拓展公益诉讼检察职能，推动形成个人信息保护多元共治新格局。积极稳妥办理涉及互联网平台企业的相关案件，加强与行政机关协作配合，健全行政执法与公益诉讼检察衔接机制，加强与法院的沟通协调，深化个人信息保护公益诉讼的制度探索，加强学习宣传，积极营造推进个人信息公益保护的法治环境。（来源：检察日报）

五、本期重要漏洞实例

➢ Microsoft 发布 2021 年 8 月安全更新

发布日期：2021-08-19

更新日期：2021-08-19

描述：8 月 10 日，微软发布了 2021 年 8 月份的月度例行安全公告，修复了其多款产品存在的 51 个安全漏洞。受影响的产品包括：Windows 10 21H1（24 个）、Windows 10 20H2 & Windows Server v20H2（25 个）、Windows 10 2004 & Windows Server v2004（25 个）、Windows 8.1 & Server 2012 R2（19 个）、Windows Server 2012（18 个）、Windows RT 8.1（18 个）和 Microsoft Office-related software（3 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，或发起拒绝服务攻击等。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	最高严重等级和漏洞影响	受影响的软件
CVE-2021-36936	**Windows Print Spooler 远程代码执行漏洞**	严重 远程代码执行	Server, version 20H2 Server, version 2004 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2021-36947	**Windows Print Spooler 远程代码执行漏洞**	重要 远程代码执行	Server, version 20H2 Server, version 2004 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2021-34483	**Windows Print Spooler 权限提升漏洞**	重要 特权提升	Server, version 20H2 Server, version 2004 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2021-26424	**Windows TCP/IP 远程代码执行漏洞**	严重 远程代码执行	Server, version 20H2 Server, version 2004 Server 2019 Windows 10

			Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2021-36948	**Windows Update Medic Service 提升权限漏洞**	重要 特权提升	Server, version 20H2 Windows 10 Server, version 2004 Server 2019
CVE-2021-36934	**Windows 权限提升漏洞**	重要 特权提升	Windows 10
CVE-2021-26432	**Windows Services for NFS ONCRPC XDR Driver 远程代码执行漏洞**	严重 远程代码执行	Server, version 20H2 Server, version 2004 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2021-36942	**Windows LSA 欺骗漏洞**	重要 欺骗	Server, version 20H2 Server, version 2004 Server 2019 Server 2016 Server 2012 R2 Server 2012
CVE-2021-34535	**Remote Desktop Client 远程代码执行漏洞**	严重 远程代码执行	Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2021-34480	**Scripting Engine 内存破坏漏洞**	严重 远程代码执行	Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2021-34478	**Microsoft Office 远程代码执行漏洞**	重要 远程代码执行	365 Apps Enterprise Office 2019

来源：https://msrc.microsoft.com/update-guide/releaseNote/2021-Aug

➢ Linux kernel 内存错误引用漏洞

发布日期：2021-05-26
更新日期：2021-08-26
受影响系统：
Linux kernel
描述：

CVE(CAN) ID: CVE-2020-25670
Linux kernel 是美国 Linux 基金会的开源操作系统 Linux 所使用的内核。
Linux kernel 的 llcp_sock_bind()存在内存错误引用漏洞。攻击者可利用该漏洞导致特权升级。
<**>
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://wordpress.org/news/2020/10/wordpress-5-5-2-security-and-maintenance-release/

➢ IBM Spectrum Scale 权限提升漏洞

发布日期：2021-05-25
更新日期：2021-08-26
受影响系统：
IBM Spectrum Scale 5.1.0.1
描述：

CVE(CAN) ID: CVE-2021-29708
IBM Spectrum Scale 是美国 IBM 公司的一套基于 IBM GPFS（专为 PB 级存储管理而优化的企业文件管理系统）的可扩展的数据及文件管理解决方案。该产品支持帮助客户减少存储成本，同时提高云、大数据和分析环境中的安全性和管理效率等。
IBM Spectrum Scale 5.1.0.1 版本存在权限提升漏洞。本地攻击者可通过访问 GUI pod 容器来获取敏感的加密密钥，从而可以提升权限。
链接：https://www.ibm.com/support/pages/node/6455629
*>
建议：

厂商补丁：
IBM

IBM 已经为此发布了一个安全公告（6455629）以及相应补丁：

6455629：Security Bulletin: A vulnerability in IBM Spectrum Scale that could allow a local attacker which has access to the GUI pod can ssh to the core pods as a privileged user (CVE-2021-29708)
链接：https://www.ibm.com/support/pages/node/6455629

➢ Adobe Acrobat Reader DC 越界读取漏洞

发布日期：2021-05-11
更新日期：2021-08-25
受影响系统：
Adobe Acrobat Reader DC <= 2021.001.20155
Adobe Acrobat Reader DC <= 2020.001.30025
Adobe Acrobat Reader DC <= 2017.011.30196
描述：

CVE(CAN) ID: CVE-2021-28551
Adobe Reader 是美国奥多比（Adobe）公司的一套 PDF 文档阅读软件。
Acrobat Reader DC 2021.001.20155 及之前版本、2020.001.30025 及之前版本和 2017.011.30196 及之前版本存在越界读取漏洞。未经身份认证的攻击者可利用该漏洞执行任意代码。
链接：https://helpx.adobe.com/security/products/acrobat/apsb21-29.html
建议：

厂商补丁：

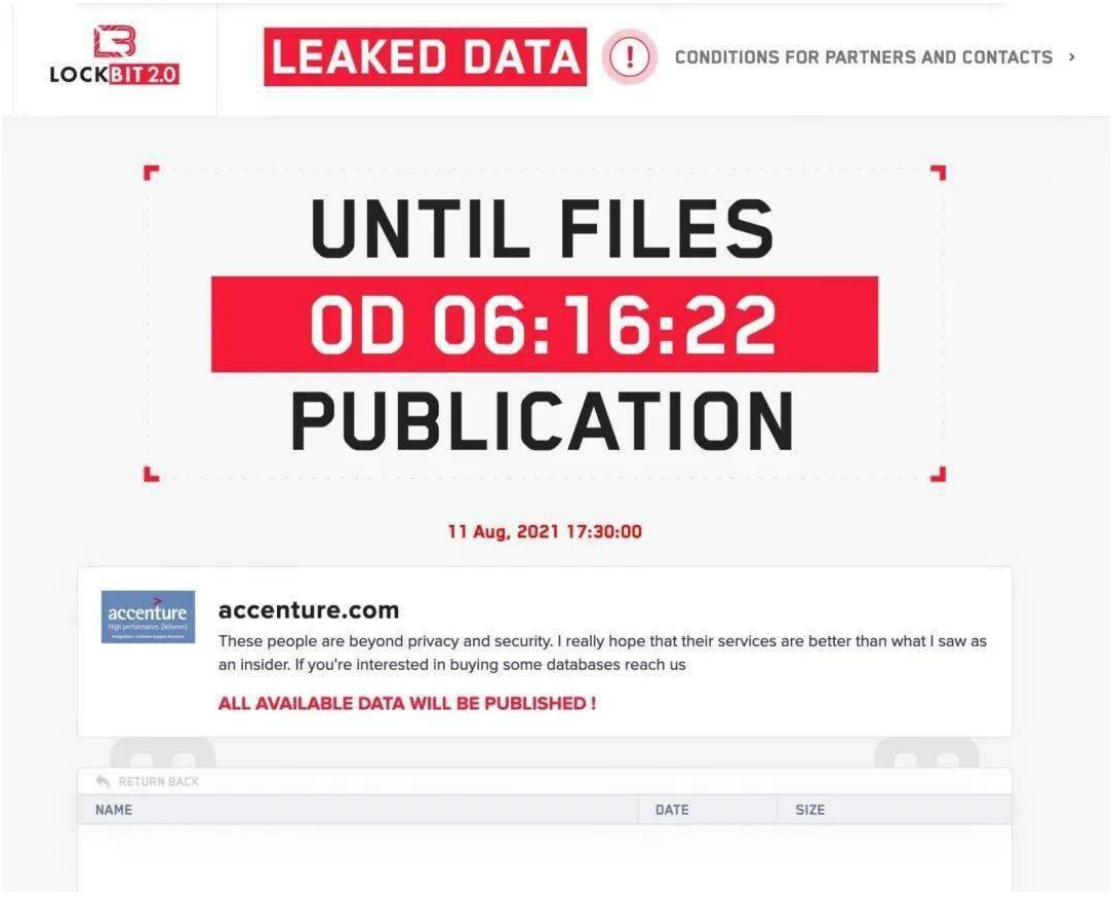
Adobe

Adobe 已经为此发布了一个安全公告（APSB21-29）以及相应补丁:
APSB21-29：Security update available for Adobe Acrobat and Reader | APSB21-29
链接：https://helpx.adobe.com/security/products/acrobat/apsb21-29.html

六、本期网络安全事件

➢ 埃森哲遭勒索攻击 要求支付 5000 万美元赎金

2021 年 8 月 12 日，一个黑客团伙 10 日晚称已使用勒索软件攻击全球知名管理和信息咨询公司埃森哲公司。**但该公司表示，勒索攻击没有影响到公司正常运营，已使用备份副本顺利恢复了受到影响系统。**埃森哲是一家以服务于汽车、银行、政府、技术、能源、电信等众多行业而闻名的 IT 巨头。埃森哲市值 443 亿美元，是全球最大的科技咨询公司之一，在 50 个国家/地区拥有约 569,000 名员工。



这次事件的曝光，源自勒索软件团伙 LockBit 在暗网博客上的公告。LockBit 团伙宣称，从埃森哲窃取了 6TB 的数据，并要求支付 5000 万美元的赎金。威胁行为者声称已通过公司“内部人员”访问埃森哲的网络。熟悉此次攻击的消息人士说，埃森哲已经向至少一家 CTI 供应商确认了勒索软件攻击，这家 IT 服务提供商也在通知更多客户。

就在 LockBit 团伙泄密网站的倒计时归零之后，LockBit 团伙如约泄露了埃森哲的文件，经过粗略审查，这些文件似乎包括埃森哲产品的小册子、员工培训课程和各种营销材料。泄

露的文件中似乎没有包含任何敏感信息。

美国布利平计算机网站以网络安全情报企业“哈得孙岩石”公司为消息源报道，埃森哲大约 2500 台供雇员和合伙人使用的计算机遭黑客攻击。

按照美国媒体说法，“锁定比特”2019 年 9 月发起首次网络攻击，迄今数以千计的组织和企业遭受攻击，包括印度媒体巨头印度报业托拉斯 LockBit 勒索团伙在近期活动频繁，该团伙在今年 6 月份更新了 2.0 版本。该勒索团伙公开招募合作伙伴，试图收买招募内部人员为他们提供访问公司网络的权限，作为回报，这些“内部人员”将会获得数百万美元的报酬。

（来源：互联网综合整理）

➢ 遭黑客攻击美电信巨头 T-Mobile 超 1 亿用户数据泄露

2021 年 8 月 15 日，美国电信巨头 T-Mobile 周日表示，该公司正在调查一个在线论坛帖子上的爆料。该帖子称，超过 1 亿用户的个人数据已被泄露。T-Mobile 是美国第三大移动通信运营商，其前两大股东分别为占股 43%的德国电信和占股 24%的软银集团，截至 2021 年第一季度拥有约 1.034 亿客户。

T-Mobile 发言人在一份声明中表示：“我们已经注意到一个地下论坛的爆料，并正在积极调查其是否属实。我们目前没有任何额外的信息可以分享。”

总部位于美国的数字媒体 Vice 首先报道了这起事件。根据 Vice 旗下科技频道 Motherboard 的报道，该论坛的帖子没有提到 T-Mobile，但黑客们声称他们已经获得了超过

1 亿人的数据，这些数据来自 T-Mobile 的服务器。这些数据包括社会保险号、电话号码、姓名、实际地址和驾照信息等信息。

据报道，黑客想要 6 个比特币(约 27 万美元)，以换取其中的一部分数据，包含 3000 万个社会安全号码和驾照的数据，而其余数据则将通过私下渠道出售。黑客还表示，T-Mobile 已经发现了违规行为，他们现在已经无法访问该公司的后门服务器，但声称在那之前就已对用户数据进行了备份。

2021 年 8 月 27 日， T-Mobile 承认，一名黑客窃取了超过 5000 万用户的数据。 这名负责入侵 T-Mobile 公司系统的黑客美国人约翰 • 宾斯（John Binns）表示，这家运营商松懈的安全措施，让他得以进入一个记录缓存，其中包含 5000 多万人用户，而且还在不断增加。这位年轻的黑客说他这样做是为了引起注意。 “制造关注是目标之一”他写道，但拒绝透露自己是否出售了任何被盗数据，或者他是否因此获得报酬。

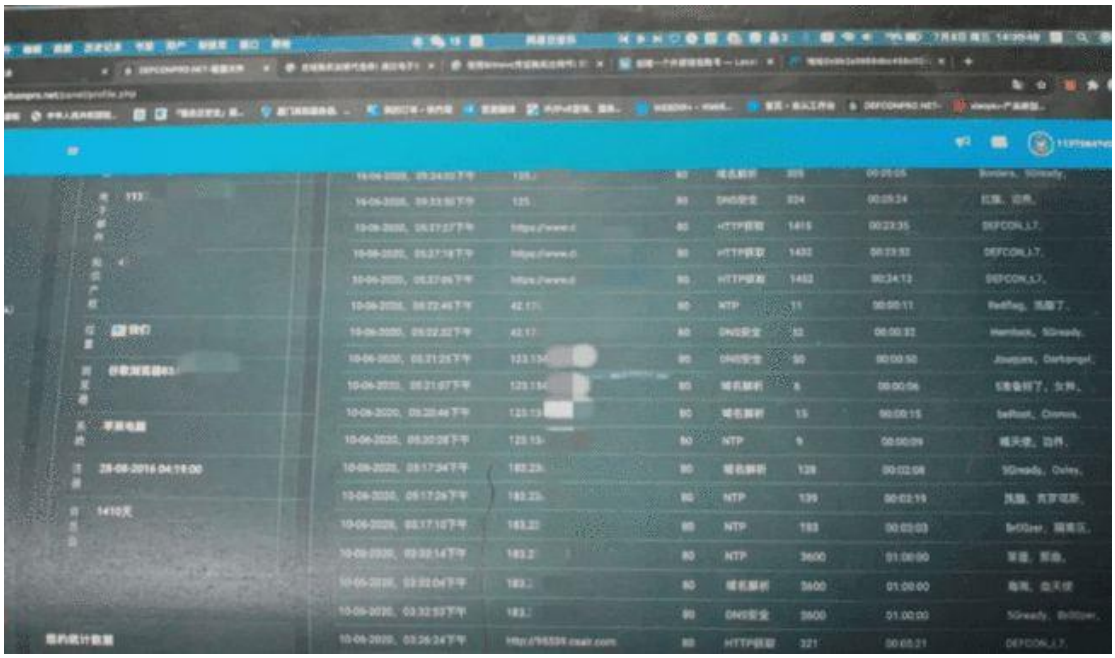
T-Mobile 则表示：正在采取措施来挽救本次数据泄露事件，包括给预估提供 2 年的免费账户保护服务；建议所有 T-Mobile 后付费客户主动更改密码；为后付费客户提供帐户接管保护功能，从而使客户帐户更难以被欺诈性地移植和窃取。（来源：财联社）

➢ 17 岁少年因购票难攻击南航购票系统 获刑四年!

2021 年 8 月 16 日，广东广州市中级人民法院曝光的一起案件，引发热议。一 17 岁小伙，利用黑客手段，让为 5000 余万用户提供服务的航空系统“停摆”4 个小时。而他的下场，是被判处有期徒刑四年。

据了解，2020 年 6 月初，17 岁的小陈因新冠疫情被强制留滞在国外疫情重灾区。在境外无法买到回国机票，他产生了不满情绪。冲动之下，他在境外网站购买攻击套餐，利用 DDOS(黑客通过远程控制服务器或计算机等资源，对目标发动高频服务请求，使目标服务器因来不及处理海量请求而瘫痪)等攻击手段，多次、持续攻击南航客票等计算机系统。

此次黑客入侵，航空公司对外服务网络全部瘫痪。包括客票业务、微信直播平台销售、机场旅客服务、飞行、运控在内的信息系统均无法正常运作，为 5000 余万用户提供服务的客票等计算机系统在这四小时内完全停摆。给航空公司造成巨大经济损失与负面网络舆论评价。2020 年 7 月，小陈回国后在广州一家酒店办理解除隔离手续时，被公安机关抓获。经过审判，广州白云法院判决小陈犯破坏计算机信息系统罪，判处有期徒刑四年。



法院：构成破坏计算机信息系统罪

广州市白云区人民法院一审认为，小陈无视国家法律，违反国家规定，对计算机信息系统功能进行干扰，造成计算机信息系统不能正常运行，后果特别严重，其行为已构成破坏计算机信息系统罪。

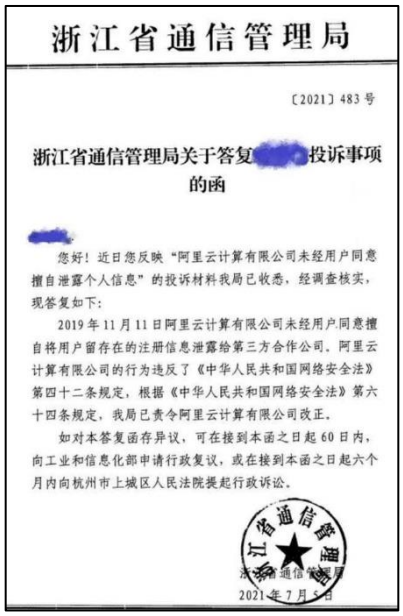
小陈犯罪时已满十六周岁不满十八周岁，依法应当减轻或者从轻处罚。综合考虑小陈犯罪行为的性质、情节、危害后果及认罪态度，判决小陈犯破坏计算机信息系统罪，判处有期徒刑四年;缴获的作案工具笔记本电脑一台予以没收。

一审宣判后，小陈不服判决，提起上诉。广州市中级人民法院经审理后裁定：驳回上诉，维持原判。值得注意的是，据小陈供述，其上完小学三年级后便辍学打工，自 15 岁起自学数字货币开发、大数据、区块链技术、人工智能。本是一名努力上进的青少年，但却因为图一时之快“泄愤”，触犯了法律，耽误了大好前程。（来源：中国青年报）

➢ 阿里云泄漏用户个人信息 当日阿里巴巴收跌超 3%

2021 年 8 月 23 日，截至当日收盘，阿里港股跌 3.67%，报 152.1 港元，总市值 32986 亿港元。今日早些时候，网络流传一份浙江省通信管理局 7 月 5 日对投诉人的答复函，内容为此前阿里云计算有限公司未经用户同意擅自将用户留存的注册信息泄露给第三方合作公司。

浙江省通信管理局答复函显示：经调查核实，2019 年 11 月 11 日阿里云计算有限公司未经用户同意擅自将用户留存的注册信息泄露给第三方合作公司，阿里云计算有限公司的行为违反了《中华人民共和国网络安全法》第四十二条规定，根据《中华人民共和国网络安全法》第六十四条规定，我局已责令阿里云计算有限公司改正。



浙江省通信管理局

〔2021〕483 号

浙江省通信管理局关于答复[redacted]投诉事项的函

[redacted]

您好！近日您反映“阿里云计算有限公司未经用户同意擅自泄露个人信息”的投诉材料我局已收悉，经调查核实，现答复如下：

2019 年 11 月 11 日阿里云计算有限公司未经用户同意擅自将用户留存在的注册信息泄露给第三方合作公司，阿里云计算有限公司的行为违反了《中华人民共和国网络安全法》第四十二条规定，根据《中华人民共和国网络安全法》第六十四条规定，我局已责令阿里云计算有限公司改正。

如对本答复函存异议，可在接到本函之日起 60 日内，向工业和信息化部申请行政复议，或在接到本函之日起六个月内向杭州市上城区人民法院提起行政诉讼。

浙江省通信管理局

2021 年 7 月 5 日

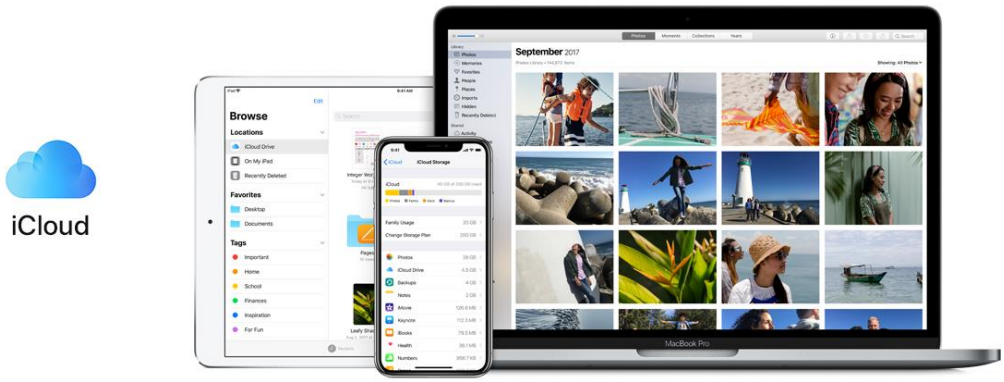
阿里云方面向媒体确认了该消息，称根据自查，该投诉事件应为 2019 年双 11 前后，阿里云一名电销员工违反公司纪律，利用工作便利私下获取客户联系方式，并透露给分销商员工，从而引发客户投诉。

阿里云方面表示：公司严禁员工向第三方泄露用户注册信息，已根据公司制度对该事件进行严肃处理，并遵照浙江省通信管理局要求积极整改，对人员管理层面上的不足进行强化改进。感谢大家的监督批评。（来源：央视新闻）

➢ 微软云平台因默认配置不当暴露 3800 万条客户数据

2021 年 8 月 24 日，据外媒报道，许多公司都在使用微软的 Power App 平台，由于默认安全设置较弱，所以这意味着 3800 万份记录的敏感数据向公众公开了好几个月。Upguard

进行的调查显示，Power App 用户中有相当多的人没有保护自己的数据库。进一步的调查显示，这个问题是由薄弱的默认安全设置造成的，如果用户不采取手动操作数据就会暴露在外面。



根据 Wired 的一份报告，美国航空公司、福特公司、纽约市公立学校和多个州的 COVID-19 接触者追踪数据库等来源的数据都被暴露。Upguard 最初的发现是在 2021 年 5 月，但微软的修复程序直到 8 月才全面推出。

UpGuard 负责网络研究的副总裁 Greg Pollock 表示：“我们发现其中一个被错误配置为暴露数据，我们从没听说过这种情况，我们想，这是一次性问题，还是一个系统性问题？由于 Power Apps 门户产品的工作方式，所以很容易快速进行调查。我们发现有很多这样的东西暴露在外。这是疯狂的。”

Upguard 开始调查大量的 Power App 门户网站，这些网站本应是私有的--甚至是微软开发的应用也存在配置错误的情况。然而，尽管这些数据是向公众开放的，但据知没有任何数据被泄露。问题的核心在于默认的安全设置。比如在设置 Power App 和连接 API 时，平台默认使相应的数据可以公开访问。由于 8 月份的更新，Power Apps 将默认设置安全设置以保护数据隐私。虽然 Upguard 努力跟公开敏感数据的平台进行沟通，但安全问题的规模太大、无法涵盖每一家企业。

“安全的默认设置非常重要，”开放加密审计项目(Open Crypto Audit Project)主任 Kenn White 指出：“当一个模式出现在使用特定技术构建的面向网络的系统中而该系统仍配置错误时就会出现非常严重的问题。如果来自不同行业和技术背景的开发者继续在一个平台上犯同样的错误，那么这个平台的创造者就应该受到关注。”

据悉，暴露的数据包括几个 COVID-19 接触者追踪平台、疫苗接种注册、工作申请门户和员工数据库。从社会安全号码到姓名和地址的所有信息都留在了开放的数据库中。

Upguard 再次表示，目前还没有任何数据被泄露。Microsoft Power 应用的安全设置问题跟该领域的许多其他平台的问题相呼应。像亚马逊和 Google 这样的公司经常也面临默认设置不佳而导致数据泄露的问题。（来源：cnBeta）

➢ 因违反信用信息采集等规定，交行、华夏、兴业被罚 553 万

2021 年 8 月 20 日，2021 年 8 月 20 日，中国人民银行发布的行政处罚公示信息显示，交通银行、华夏银行、兴业银行因违反信用信息采集、提供、查询及相关管理规定，被罚款合计 553 万元。

此外，时任交通银行太平洋信用卡中心风险管理和控制部操作风险管理团队经理、资深综合管理顾问的沈奕栋，对交通银行“违反信用信息采集、提供、查询及相关管理规定”违法违规行为负有责任，被罚款 7 万元。

序号	当事人名称	行政处罚决定书文号	违法行为类型	行政处罚内容	作出行政处罚决定机关名称	作出行政处罚决定日期	备注
1	交通银行股份有限公司	银罚字〔2021〕23号	违反信用信息采集、提供、查询及相关管理规定。	罚款62万元	中国人民银行	2021年8月13日	
2	沈奕栋（时任交通银行太平洋信用卡中心风险管理和控制部操作风险管理团队经理、资深综合管理顾问）	银罚字〔2021〕24号	对交通银行以下违法违规行为负有责任：违反信用信息采集、提供、查询及相关管理规定。	罚款7万元	中国人民银行	2021年8月13日	

序号	当事人名称	行政处罚决定书文号	违法行为类型	行政处罚内容	作出行政处罚决定机关名称	作出行政处罚决定日期	备注
1	华夏银行股份有限公司	银罚字〔2021〕25号	违反信用信息采集、提供、查询及相关管理规定。	罚款486万元	中国人民银行	2021年8月13日	

序号	当事人名称	行政处罚决定书文号	违法行为类型	行政处罚内容	作出行政处罚决定机关名称	作出行政处罚决定日期	备注
1	兴业银行股份有限公司	银罚字〔2021〕26号	违反信用信息采集、提供、查询及相关管理规定。	罚款5万元	中国人民银行	2021年8月13日	

值得一提的是，同日，第十三届全国人大常委会第三十次会议表决通过《中华人民共和国个人信息保护法》，自 2021 年 11 月 1 日起施行。

《中华人民共和国个人信息保护法》明确规定：违反规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务;拒不改正的，并处一百万元以下罚款;对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照;对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。（来源：中国人民银行）