国盟信息安全通报

2020 年 10 月 25 日第 227 期

全国售后服务中心

国盟信息安全通报

（第 227 期）

国际信息安全学习联盟

2020 年 10 月 25 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 372 个，其中高危漏洞 124 个、中危漏洞 180 个、低危漏洞 68 个。漏洞平均分值为 5.66。本周收录的漏洞中，涉及 0day 漏洞 153 个（占 41%），其中互联网上出现“WordPress Colorbox Lightbox 跨站脚本漏洞、WebBuilder SQL 注入漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 5332 个，与上周（3670 个）环比增加 45%。

主要内容

一、概述 4
二、安全漏洞增长数量及种类分布情况 4
➢漏洞产生原因（2020 年 10 月 11 日—2020 年 10 月 25）.....4
➢漏洞引发的威胁（2020 年 10 月 11 日—2020 年 10 月 25）.....5
➢漏洞影响对象类型（2020 年 10 月 11 日—2020 年 10 月 25）.....5
三、安全产业动态 6
➢落实“四个坚持”原则要求 守护网络家园清朗安全.....6
➢详解个人信息保护法草案：国家机关履职应遵循告知同意原则.....8
➢Gartner 发布 2021 年重要战略科技趋势.....12
➢提升网络安全从业人员的职业意识和专业化水平.....15
四、政府之声 20
➢《中华人民共和国个人信息保护法（草案）》发布.....20
➢ 十四部门印发 《2020 网络市场监管专项行动（网剑行动）方案的通知》.....24
➢《中华人民共和国未成年人保护法修订》2021 年 6 月 1 日施行.....26
➢《互联网用户公众账号信息服务管理规定（修订草案征求意见稿）》发布.....27
五、本期重要漏洞实例 28
➢Microsoft 发布 2020 年 10 月安全更新.....28
➢Linux kernel 内存破坏和读取溢出漏洞.....30
➢Cisco IOS XE 任意代码执行漏洞.....31
➢Gitlab runner 命令注入漏洞.....31
六、本期网络安全事件 32
➢全球交易所遭遇水逆月 接二连三发生宕机故障.....32
➢黑客控制服务器 103 台，被判 3 年缓刑 4 年罚金 15000.....33
➢希腊电信公司遭黑客攻击 数百万个电话数据被窃取.....35
➢美国 1.86 亿选民数据在暗网被黑客出售，FBI 介入调查.....36
➢六家银行因侵害个人信息被罚逾 4000 万元.....37
➢英国航空因数据泄露的巨额罚款 减至 2000 万英镑.....39

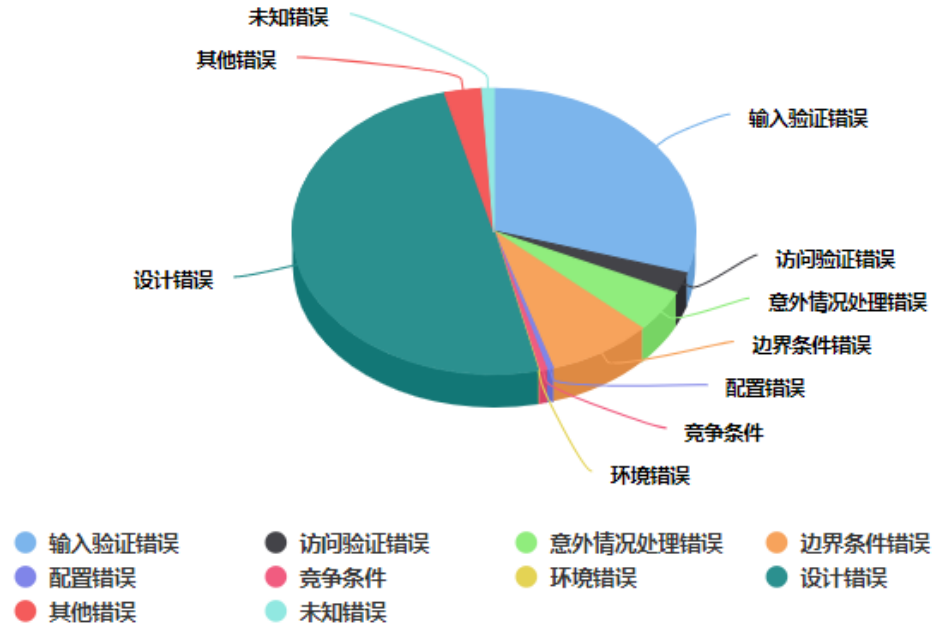
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

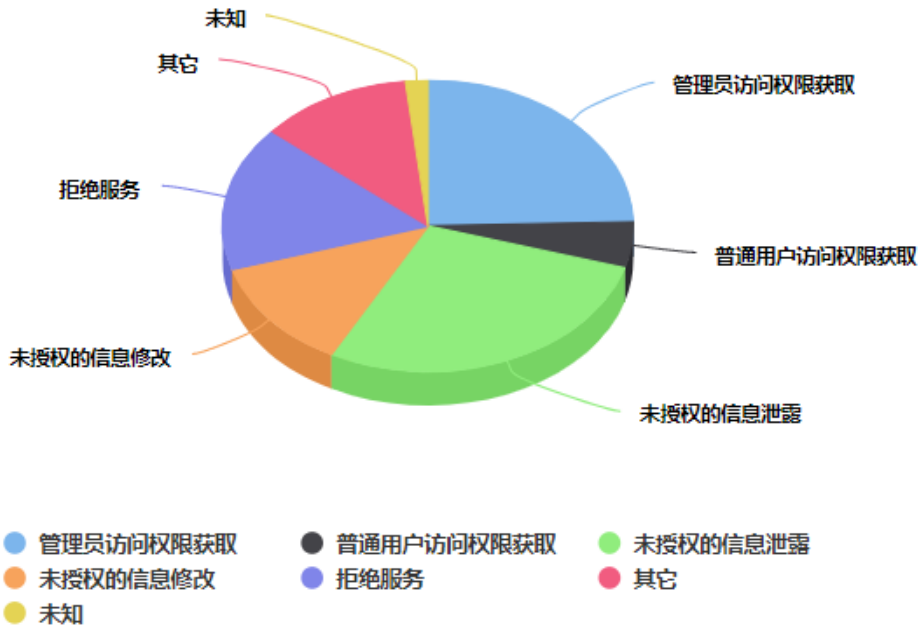
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 372 个，其中高危漏洞 124 个、中危漏洞 180 个、低危漏洞 68 个。漏洞平均分值为 5.66。本周收录的漏洞中，涉及 0day 漏洞 153 个（占 41%），其中互联网上出现“WordPress Colorbox Lightbox 跨站脚本漏洞、WebBuilder SQL 注入漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 5332 个，与上周（3670 个）环比增加 45%。

二、安全漏洞增长数量及种类分布情况

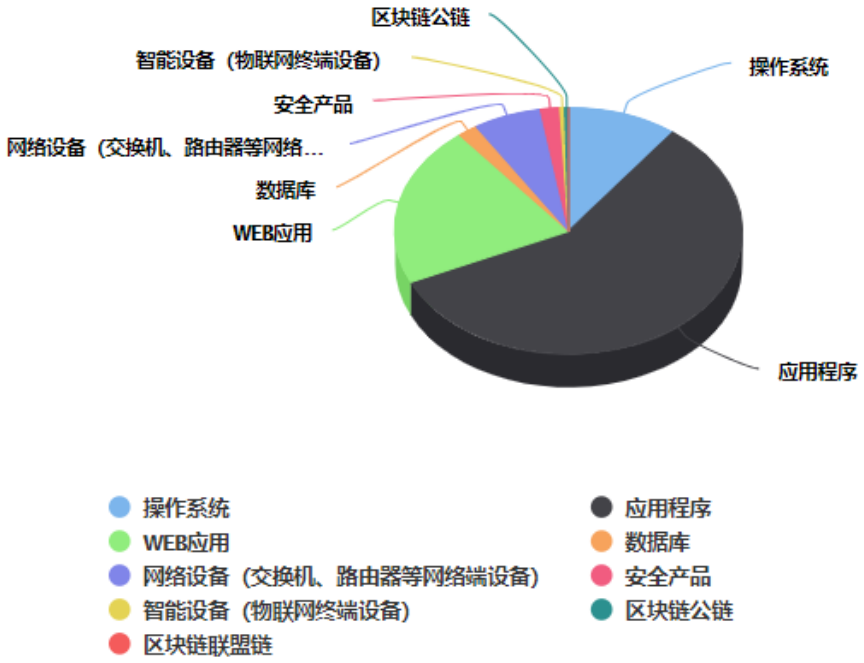
➢ **漏洞产生原因（2020 年 10 月 11 日—2020 年 10 月 25）**



➢ 漏洞引发的威胁（2020 年 10 月 11 日—2020 年 10 月 25）



➢ 漏洞影响对象类型（2020 年 10 月 11 日—2020 年 10 月 25）



三、安全产业动态

➢ 落实“四个坚持”原则要求 守护网络家园清朗安全

“2020 年国家网络安全宣传周于 9 月 14 日至 20 日在全国范围内统一开展。作为国家网络安全工作的重要组成部分，网安周始终植根人民立场、呼应人民需求、顺应人民期待，立足于提升亿万网民的网络安全意识和知识技能，致力于让互联网更好造福国家和人民，开展了系列卓有成效的工作宣传和知识普及工作，为推动网信事业发展打下了坚实的群众基础。

2019 年，习近平总书记对网络安全作出“四个坚持”的重要指示，强调要保障个人信息安全，维护公民在网络空间的合法权益。总书记的指示为我们做好网安周工作指明了方向、提供了根本遵循。

网信事业发展关乎国家前途、社会安全和民众利益。发展网信事业，必须牢牢树立以人民为中心的发展理念，把增进人民福祉作为出发点和落脚点，把习近平总书记“四个坚持”的重要指示贯穿于网信工作的全过程、各领域，落实到网安周各项工作中，发动全社会的力量共同守护网络空间安全和精神家园清朗。

守护网络家园清朗安全，必须坚持“网络安全为人民、网络安全靠人民”的理念。习近平总书记在网络安全和信息化工作座谈会上强调，网信事业要在践行新发展理念上先行一步，推进网络强国建设，推动我国网信事业发展，让互联网更好造福国家和人民。网络安全

为人民，要把增进人民福祉作为信息化发展的出发点和落脚点。特别是在当前受新冠肺炎疫情冲击、内外部风险挑战交织的情况下，更要发挥“互联网+”在经济转型和新旧动能转换过程中的重要推动作用，大力开展网络扶贫、数字扶贫等专项行动，切实改善民生、补齐短板弱项，把惠民、利民、富民、改善民生作为科技创新的重要方向，进一步增强人民群众在网络发展过程中的获得感、幸福感。网络安全靠人民，要发挥好企业、科研院校、专家智库等作用，健全完善社会协同和全民参与的网络综合治理体系，汇聚起全社会、各领域维护国家网络安全的澎湃力量，筑牢网络安全防护长城。

守护网络家园清朗安全，必须坚持网络安全教育、技术、产业融合发展。近些年，以云计算、大数据、人工智能为代表的新一代信息技术加速发展，向经济社会相关领域、传统行业跨界的趋势明显、融合加速。“互联网+”以信息流带动技术流、资金流、人才流、物资流，推动“互联网+教育”“互联网+医疗”“互联网+交通”等新业态新应用加速发展，为推动创新发展、转变经济发展方式、调整经济结构提供了新动能、加速器。随着产业融合进程的不断深入，万物互联的泛在接入、高效传输、海量异构信息处理和设备智能控制，以及由此引发的安全问题，对产业融合安全提出了更高要求，迫切需要转变发展理念，在推动“互联网+”发展的同时，进一步强化网络安全教育，提高全民的网络安全素养，提高企业的网络安全技术能力，同步推进技术进步、产业融合，妥善处理好网络安全与产业融合发展关系。

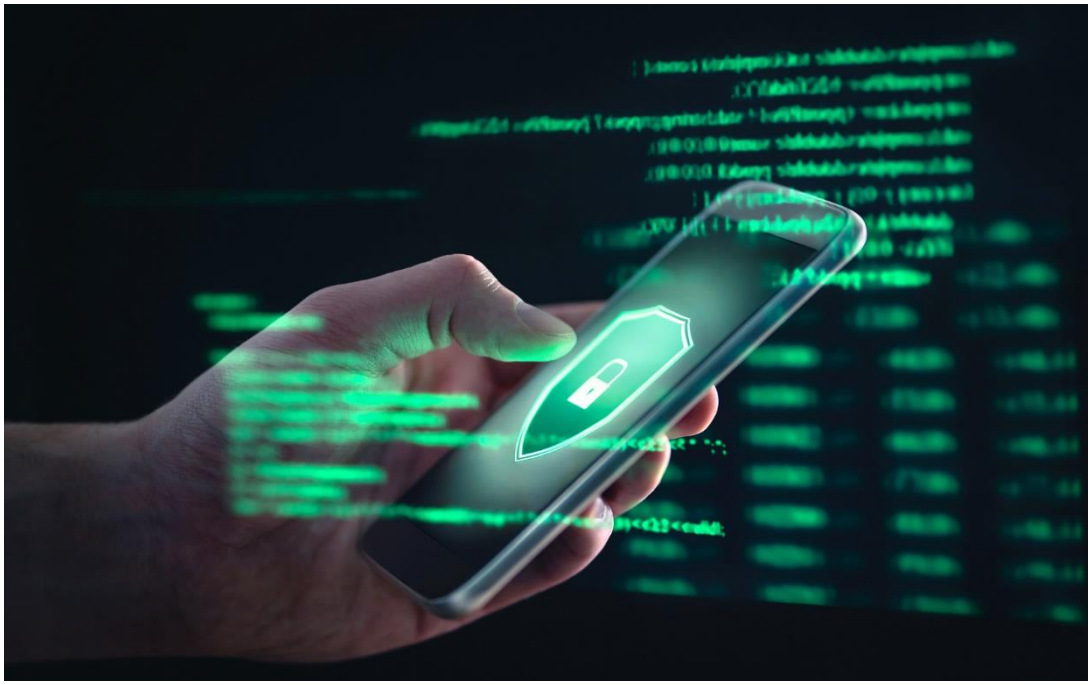
守护网络家园清朗安全，必须坚持促进发展和依法管理相统一。依法治网是网信工作的重要原则，也是健全完善网络综合治理体系的重要内容。习近平总书记指出，“网络空间不是‘法外之地’”“要坚持依法治网、依法办网、依法上网，让互联网在法治轨道上健康运行”。党的十八大以来，党中央着眼推进网络强国战略部署，出台了一系列网络安全战略纲要、发展规划、指导意见，制定出台了以《网络安全法》为代表的网信领域法律法规，基本确立了依法管网治网的“四梁八柱”。同时，随着网络新技术新应用的快速发展，以大数据、卫星互联网、区块链、5G 为代表的网络新技术加速应用，给依法管网带来许多新问题、新挑战，迫切需要我们顺应新技术新应用发展趋势，加快出台《数据安全法》《个人信息保护法》等法律。维护网络空间安全清朗，比科学立法更重的是加强网信领域严格执法、公正司法和全民守法。法律的尊严在于执行。要依法加强对网络运行主体和网民行为的监管，推动网信领域各项法律法规落地落实、生根发芽，真正为推动互联网又好又快发展提供法律保障。

守护网络家园清朗安全，必须坚持安全可控与开放创新并重。习近平总书记在全国宣传思想工作会议上强调，“要依法加强网络社会管理，加强网络新技术新应用的管理，确保互联网可管可控，使我们的网络空间清朗起来”。建设网络强国，安全是前提，可控是保障。

没有安全的网络发展和技术创新，好比脱缰的野马，奔腾咆哮，却危机四伏。维护国家网络安全，一方面，需要依法依规加强网络综合治理，提高网络空间意识形态风险防范化解和网络空间安全抵御能力，重点实施网络信息领域核心技术设备攻坚战略，千方百计扭转“卡脖子”技术受制于人的被动局面。另一方面，需要顺应信息领域技术创新发展趋势，营造开放包容的创新环境，深化科技研发投入产出和成果转化机制改革，强化科技创新体系建设，矢志不移坚持自主创新，把满足人民对美好生活的向往作为科技创新的落脚点，把惠民、利民、富民、改善民生作为科技创新的重要方向，加快构筑支撑高端引领的先发优势，为加快推动网络强国、科技强国建设作出贡献。（来源：网信中国）

➢ 详解个人信息保护法草案：国家机关履职应遵循告知同意原则

2020 年 10 月 21 日，中国人大网公开《中华人民共和国个人信息保护法（草案）》（下称“草案”）并面向社会征求意见，截止时间为 11 月 19 日。草案共八章七十条内容，包括“个人信息处理一般规定”、“敏感个人信息的处理规则”、“个人信息跨境提供的规则”等专门章节。中国社会科学院法学研究所研究员周汉华认为，草案的一大亮点在于，相比过去零碎的、片段式的立法，草案对个人信息的整个生命周期进行了一个全流程的系统设计，解决了过去几部立法都没有解决的问题。



一、从个人信息生命周期角度进行系统设计

近年来，随着网络化、数字化技术的发展，人们在享受科技技术带来的便利服务的同时，也遇到许多新的问题。其中，因个人信息保护不周带来的电信诈骗、垃圾短信、大数据杀熟等问题切实损害了民众的利益。2016 年，山东准大学生徐玉玉因个人信息泄露，被电信诈骗骗走学费 9900 元，郁结于心，最终导致心脏骤停不幸离世。

个人信息保护问题越来越被大众关注，社会各方面也一直呼吁出台专门的个人信息保护法。据人大法工委介绍，本届以来，全国人大代表共有 340 人次提出 39 件相关议案、建议，全国政协委员共提出相关提案 32 件。

针对个人信息保护问题，虽然一直没有专门立法，但在刑法、消费者权益保护法、网络安全法、民法典中都有相关规定。“但（它们）都不是集中的全面的规定。” 清华大学法学院教授、副院长程啸强调，个人信息保护法是个人信息保护领域中最为全面最为集中的法律规范，有了这样一部法律，我国就真正形成了以民法典、个人信息保护法、为核心的，相关领域特别法为辅助的科学合理的个人信息保护法律规范体系。

“个人信息保护法不仅将（其他法律中）零散的条款，特别是它们背后的思想整合起来，更会归管这些条款尚未涉及的地方。”中国法学会民法典编纂领导小组侵权责任编召集人、中国人民大学法学院教授张新宝表示，它还积极回应了信息技术，特别是互联网应用对社会生活的影响，在强化对公民个人信息特别是私密信息保护的同时，为信息产业界划定合法合规创新发展经营的边界。

针对草案的亮点，中国社会科学院法学研究所研究员周汉华认为可归纳为一个“内”和一个“外”。“内”是指草案以个人权利为核心理念，体现在草案的整个制度构造中，把知情同意原则作为一个主线。

“过去好几部法律都规定了个人信息保护的内容，但是一直没有点出个人信息权这么一个概念。”他表示，这一次在立法说明当中，明确提出个人权利这个概念，意味着个人在现代社会是可以控制自己的信息的，这是国际社会的普遍经验，也就是草案内核的亮点。

在个人信息处理活动中，个人拥有哪些权利？草案对此进行了明确，包括知情权、决定权、查询权、更正权、删除权等。

“外”则是指和过去零碎的、片段式的立法相比，草案对个人信息的整个生命周期进行了一个全流程的系统设计。“从采集到使用，到安全保护、跨境提供，再到敏感个人信息的处理、管理部门的确定和法律责任……这是过去的几部立法都没有解决的问题。”周汉华说。

二、回应个性化推送、人脸识别等社会热点问题

自动化决策，指的是技术系统在没有人工干预的情况下自动作出决策。互联网平台基于

用户画像进行的“千人前面”“猜你喜欢”的个性化推送，就是一种典型的自动化决策。

草案第二十五条规定，通过自动化决策方式进行商业营销、信息推送，应当同时提供不针对其个人特征的选项。

全国人大常委会委员吕薇对这条规定印象很深，她认为，自主化决策有利有弊。一方面，个性化信息流可以帮助消费者快速从海量商品信息中找到所用、所需的商品和信息；另一方面，也存在差别化定价、大数据杀熟等现象。

因此她提出，第二十五条的关键是，在推送方式上，不能是强制性的推送，应该允许消费者选择是否接受推送，并为消费者提供关闭选项。

前不久，《个性化展示安全与合规报告（2020）》。报告发现，常用20款App中有八成被测App的个性化展示用户友好程度处于中等以下水平，绝大部分App都要经过五次以上甚至上十次跳转才能找到关闭按钮。

草案还针对人脸识别这一社会热点问题做出了回应。第二十七条明确，在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、个人身份特征信息只能用于维护公共安全的目的，不得公开或者向他人提供；取得个人单独同意或者法律、行政法规另有规定的除外。

记者注意到，一些商场门店已经开始使用人脸识别设备进行客流分析；疫情期间，多地小区也开始使用人脸识别设备进行防控。但上述场景能否上升到公共安全的高度，各方看法不一。对于这条规定，吕薇认为，应该进一步明确“谁可以安装图像采集和个人身份识别设备，需要什么样的批准程序，由谁来批准”等问题。同时，要注意防范过度收集，保障被收集的信息不被用于公共安全以外的用途。

周汉华则表示，该条规定回应了现在大家比较关注的生物信息的采集问题，尤其是人脸识别，社会各界的关注度比较高。“把维护公共安全作为前提条件，应该说对于可能发生的（人脸识别）滥用现象能够产生遏制效应。”

去年10月，因为不愿意被强制刷脸，浙江某大学特聘副教授郭兵将杭州野生动物世界告上法庭。案件引发广泛关注，被业内人士称为“国内人脸识别第一案”。

周汉华以此案为例指出，杭州野生动物世界显然不是为了公共安全考虑，而是为了提高效率，就不具备强制使用人脸识别的必要性。他认为，草案会对法院裁判该案起到很强的指导性。不过，实际效果如何“还是要取决于法规的执行和实施”。他说，公共安全和公共利益一样，是一个伸缩性很强的概念，小区和商场可能都认为自己跟公共安全有关。“怎样使得公共安全真正落实而不流于形式，就需要社会各界的共同对话。”

三、处罚对大型公司和机构具有震慑力

据中国互联网络信息中心于 9 月份发布的第 46 次《中国互联网络发展状况统计报告》显示，截至 2020 年 6 月，我国网民规模为 9.40 亿，网站数量为 468 万个，App 数量有 359 万个。毫无疑问，网络已成为生产生活的新空间、经济发展的新引擎、交流合作的新纽带。

然而，一些企业、机构甚至个人，从商业利益等出发，随意收集、违法获取、过度使用、非法买卖个人信息，利用个人信息侵扰人民群众生活安宁、危害人民群众生命健康和财产安全等问题仍十分突出。

对此，草案第六十二条规定，违反本法规定处理个人信息，或者处理个人信息未按照规定采取必要的安全保护措施的，情节严重的，由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。

记者梳理发现，《反垄断法》是我国第一部采用上年度营业额百分比作为处罚基准的法律，《个人信息保护法》可能成为第二部。上一年度营业额百分之五的罚款对于大型公司和机构来说，无疑极具震慑力。

在周汉华看来，这条规定将是未来审议中的焦点问题。他指出，五千万和上一年度营业额百分之五大大提高了现有的罚款额度，“会不会有市场主体认为太高？还是说力度还不够？实施当中是不是能够落得了地？我想会是一个大家广泛关注的问题。”

国家机关如何处理个人信息？草案第二章第三节设立专节— “国家机关处理个人信息的特别规定”。

第三十五条规定，国家机关为履行法定职责处理个人信息，应该依照本法规定向个人告知并取得同意。第三十六规定，国家机关不得公开或者向他人提供其处理的个人信息，法律、行政法规另有规定或者取得个人同意的除外。

周汉华认为，草案中的这一章节也是亮点之一。他表示，该规定体现了对国家机关和市场主体同等对待的原则，是规则平等的一个表现，有重要意义。尤其是现在国家机关泄露或者滥用个人信息的情况的确存在，所以规定也具有现实意义。

此外，草案中的第三章“个人信息跨境提供的规则”也是一大看点。华东政法大学教授、互联网法治研究院院长高富平认为这部分细化了个人信息跨境传输的有关要求，也为个人信息出境提供了多渠道的方式。比如，第四十一到四十三条基于国家安全的要求，分别从司法协助、限制措施和对等措施的角度进行了规定。

谈及个人信息保护法的定位，程啸告诉南都记者，这部法律本身并非单纯的民事特别法，而是一部运用民事、行政等综合性手段对于个人信息加以保护，对于自然人个人信息权益、

信息自由、公共利益等多重利益关系加以协调的法律。（来源：隐私护卫队）

➢ Gartner 发布 2021 年重要战略科技趋势

全球领先的信息技术研究和顾问公司 Gartner 于今日发布企业机构在 2021 年需要深挖的重要战略科技趋势。分析师们在本周举行的 Gartner IT Symposium/Xpo 大会美洲站虚拟会议上展示了自己的发现。Gartner 研究副总裁 Brian Burke 表示：“各企业职能部门对运营韧性的需求从未像现在这样强烈。首席信息官们正在努力适应不断变化的情况，设计未来的业务。这就需要企业机构具有不断重组与改革的可塑性。Gartner 2021 年重要战略科技趋势可实现这种可塑性。

“企业机构正在从应对新冠疫情转向推动增长，因此它们必须关注形成今年主流趋势的三个主要领域：以人为本、位置独立性和韧性交付。这些趋势在组合后的整体影响大于它们各自的独立影响，并且专注于满足全球各地的社会与个人需求来实现最佳交付。”

2021 年重要战略科技趋势具体如下：

行为互联网（Internet of Behaviors）

行为互联网（IoB）不断涌现，许多技术都在捕获并使用人们日常生活中的“数字尘埃”。IoB 汇集了面部识别、位置跟踪和大数据等当前直接关注个人的技术，并将结果数据与现金购买或设备使用等相关的行为事件相关联。

企业机构使用该数据来影响人的行为。例如为了在疫情期间监控对健康规定的遵守情况，企业机构可以通过使用 IoB 计算机视觉来查看员工是否戴着口罩或通过热成像来识别发热者。Gartner 预测，到 2025 年末，全球一半以上的人口将至少参加一项商业或政府的 IoB 计划。虽然 IoB 在技术上可成为可能，但社会各界将对各种影响行为的方法展开广泛的伦理和

社会学讨论。

全面体验（Total Experience）

Burke 表示：“去年，Gartner 将多重体验定义为一种重要的战略科技趋势。而在今年，这一趋势又进一步发展成为全面体验（TX），将多重体验与客户、员工和用户体验相联系。Gartner 预计在未来三年中，提供 TX 的企业机构在关键满意度指标方面的表现将超越竞争对手。”

由于新冠疫情，移动、虚拟和分布式互动日益盛行，因此企业机构需要有 TX 策略。TX 将改善体验的各个组成部分，实现业务成果的转型。这些相互交织的体验是企业运用创新革命性体验实现差异化，从而从疫情中恢复的关键驱动力。

隐私增强计算（Privacy-Enhancing Computation）

随着全球数据保护法规的成熟，各地区首席信息官所面临的隐私和违规风险超过了以往任何时候。不同于常见的静态数据安全控制，隐私增强计算可在确保保密性或隐私的同时，保护正在使用的数据。

Gartner 认为，到 2025 年将有一半的大型企业机构使用隐私增强计算在不受信任的环境和多方数据分析用例中处理数据。企业机构应在开始确认隐私增强计算候选对象时，评估要求个人数据转移、数据货币化、欺诈分析和其他高度敏感数据用例的数据处理活动。

分布式云（Distributed Cloud）

分布式云将公有云分布到不同的物理位置，但服务的运营、治理和发展依然由公有云提供商负责。它为具有低延迟、降低数据成本需求和数据驻留要求的企业机构方案提供了一个灵活的环境，同时还使客户的云计算资源能够更靠近发生数据和业务活动的物理位置。

到 2025 年，大多数云服务平台至少都能提供一些可以根据需要执行的分布式云服务。Burke 先生认为：“分布式云可以取代私有云，并为云计算提供边缘云和其他新用例。它代表了云计算的未来。”

随处运营（Anywhere Operations）

随处运营是一种为全球各地客户提供支持、赋能全球各地员工并管理各类分布式基础设施业务服务部署的 IT 运营模式。它所涵盖的不仅仅是在家工作或与客户进行虚拟互动，还能提供所有五个核心领域的独特增值体验，分别是：协作和生产力、安全远程访问、云和边缘基础设施、数字化体验量化以及远程运营自动化支持。到 2023 年末，40%的企业机构将通过随处运营提供经过优化与混合的虚拟/物理客户与员工体验。

网络安全网格（Cybersecurity Mesh）

网络安全网格使任何人都可以安全地访问任何数字资产，无论资产或人员位于何处。它通过云交付模型解除策略执行与策略决策之间的关联，并使身份验证成为新的安全边界。到 2025 年，网络安全网格将支持超过一半的数字访问控制请求。

Burke 先生认为：“新冠疫情加快了耗时数十年的数字化企业变革过程。我们已经越过了一个转折点，大多数企业机构的网络资产现在都已超出传统的物理和逻辑安全边界。随着随处运营的不断发展，网络安全网状组网将成为从非受控设备安全访问和使用云端应用与分布式数据的最实用方法。”

组装式智能企业（Intelligent Composable Business）

Burke 先生表示：“为了提高效率而建立的静态业务流程非常脆弱，因此在疫情的冲击下变得支离破碎。首席信息官和 IT 领导者正在努力收拾残局，他们开始了解适应业务变化速度的业务能力有多么重要。”

智能组合型业务通过获取更好的信息并对此做出更敏锐的响应来彻底改变决策。依靠丰富的数据和洞见，未来的机器将具有更强大的决策能力。智能组合型业务将为重新设计数字化业务时刻、新业务模式、自主运营和新产品、各类服务及渠道铺平道路。

人工智能工程化（AI Engineering）

Gartner 的研究表明，只有 53%的项目能够从人工智能（AI）原型转化为生产。首席信息官和 IT 领导者发现，由于缺乏创建和管理生产级人工智能管道的工具，人工智能项目的扩展难度很大。为了将人工智能转化为生产力，就必须转向人工智能工程化这门专注于各种人工智能操作化和决策模型（例如机器学习或知识图）治理与生命周期管理的学科。

人工智能工程化立足于三大核心支柱：数据运维、模型运维和开发运维。强大的人工智能工程化策略将促进人工智能模型的性能、可扩展性、可解释性和可靠性，完全实现人工智能投资的价值。

超级自动化（Hyperautomation）

业务驱动型超级自动化是一项可用于快速识别、审查和自动执行大量获准业务和 IT 流程的严格方法。在过去几年中，超级自动化一直在持续不断地发展。而因为疫情，一切事物都被突然要求首先实现数字化，这大大增加了市场的需求。业务利益相关者所积压的需求已促使 70%以上的商业机构实施了数十种超级自动化计划。

Burke 先生表示：“超级自动化是一股不可避免且不可逆转的趋势。一切可以而且应该被自动化的事物都将被自动化。”（来源：Gartner）

➢ 提升网络安全从业人员的职业意识和专业化水平

近年来，网络安全行业快速发展，网络安全从业人员数量逐渐增多，社会影响不断增大，职业意识日益普及。所谓职业意识，指的是人们对职业活动的认知、评价、情感和态度的综合反映。随着网络安全职业化发展进程加快、国家网络安全宣传工作持续深化，公众对网络安全工作职责、这项工作的意义、价值取向以及入门的途径都有了更深的认识。为实现网络强国战略目标，充分发挥网络安全人才在经济社会发展和国家安全保障中的关键作用，有必要进一步强化网络安全职业意识，提升从业人员专业化水平，增强网络安全职业吸引力，充实网络安全人才队伍，提高国家整体网络安全保障能力。

一、网络安全职业意识日益深入人心

随着网络安全从信息技术的一个分支逐步发展为自成体系的专业领域，从业人员也经历了从探索到专精、从兼职到专职的转变，网络安全职业意识日益普及。公众对网络安全专业人员的工作任务、承担的职责，以及所做的贡献也有了更多的了解。

为适应时代需要，国家人力资源和社会保障部近年来发布了若干网络与信息安全相关职业信息：2015 年 7 月，《中华人民共和国职业分类大典》（以下简称“《职业分类大典》”）首次修订，新增“信息安全工程技术人员（职业编码 2-02-10-07）”和“网络与信息安全管理员（职业编码 4-04-04-02）”两个职业；2020 年 6 月，《职业分类大典（2015 年版）》颁布后发布的第三批新职业中设立“信息安全测试员（职业编码 4-04-04-04）”职业。网络与信息安全相关职业得到人社部门的认可，反映了国家层面高度重视在网络安全这一具有典型新产业、

新业态、新模式特点的领域推进职业化发展。

同时我们也应注意到，以发展的眼光来看，现有的网络和信息安全职业分类还远远无法满足网络安全各细分领域的人才需求，从业人员的职业化发展仍处在初级阶段。网络安全具有跨界交叉融合、知识快速更新的特点，难以在传统职业框架下形成单一、成熟且稳定的职业技能；加之我国信息化起步较晚，网络安全产业规模还比较小，还不能支撑足够细化和深化的产业分工。目前网络安全还没有的职业或职业族标准，对从业人员如何科学地分级分类、应具备何种专业知识和能力水平等问题尚未建立标准规范，各用人单位的信息安全岗位设置和能力要求各行其是，差别还比较大。公众对于真实的网络安全职责也存在一些误解，如对于从业者的工作内容，往往过于强调其中攻击渗透的一面。还有一些希望进入行业的人员仅能通过碎片化的方式了解行业相关知识和能力要求，难以对网络与信息安全知识体系进行系统的把握，对相关工作要求缺乏整体准确的认识。

二、美国发展网络安全职业的举措

1．政策法规凸显网安人才重要性

美国把网络安全人才看作战略性国家安全资源，把网安人才的短缺视为不利于国家安全和政府运行的高风险问题。为此，美国采取了大量行政和立法手段以确保人才建设的落实，为该领域工作提供充足的经费和资源保障。早在 2002 年发布的《联邦信息安全管理法（FISMA）》中就明确，政府部门负责人对网络安全工作负总责，其中就包括对本部门网络安全人才队伍建设的职责。具体要求是“确保本部门人员经过充分的培训，能够配合部门完成相关政策、规程、标准和指南的合规要求”；负责人还应“指定部门的首席信息官（CIO）或同等职位的领导负责确保满足本部门的合规要求，包括对承担重要信息安全职责的人员进行培训和监督”。美联邦政府各部门需每年由监察长（IG）对本部门 FISMA 的法律执行情况进行审计，对各项安全支出进行检查，这就确保了各部门的网络信息安全人员培训预算能够落地。据公开的数据，美联邦政府 2011 财年的 IT 安全培训支出在整体 IT 安全支出中所占比例是 2.5%，约为 3.3 亿美元。美国还于 2010 年启动了“国家网络安全教育计划（NICE）”，力图通过这一国家级的计划加强政产学各方面的合作，推进全美网络安全教育工作，培养网络安全专业人才队伍，进而消减关键基础设施中的漏洞隐患，维护美国网络空间安全。

2．标准化手段建设网安人才队伍

为了实现网络安全人才工作的规模化发展，美国高度重视人才标准的开发和应用。针对不同领域的网络安全人员，分别制定有相应的人才框架和能力要求规范。这其中，要求最高的当属美国国防部的人员标准。由于美军网络行动目标遍布全球，且存在大量跨部门、跨军

种，乃至盟国之间的跨国境联合行动，因此网络安全人才标准化建设始终是国防部网络空间能力建设的核心所在。目前，美国防部网空人员管理依据的是 DoDD 8570 号令《信息保障（IA）培训、认证和人员管理》及其配套实施手册 DoD 8570.01M《信息保障人员改进计划》。手册中对国防部所有承担信息保障（IA）职责的人员类型和级别进行了详细的划分，并对每个类型和级别的人员必须达到的基线资质要求做出了明确、硬性的规定。在民用领域，美国使用的网络安全人才标准主要是 NICE 计划主导编制的《国家网络安全人力框架（NCWF）》。该框架首次发布于 2013 年，修订后于 2017 年成为 NIST SP800-181 号国家标准。NCWF 旨在使用通用的术语来定义和描述公私领域各项网络安全工作的内容，详细描述了每个网络安全角色应承担的工作任务，以及应该具备的知识、技能和能力。

3．设立网络安全职业意识宣传周

美国在网络安全意识宣传方面，除了每年十月份的“国家网络安全意识宣传月（NCSAM）”以外，还从 2017 年开始启动了一项名为“国家网络安全职业意识宣传周（NCCAW）”的活动。前者的目的是在全美范围内提高公众的网络安全意识，后者则重点关注的是网络安全职业和其中的从业人员。NCCAW 由美国国家网络安全教育计划（NICE）牵头发起，时间约在每年 11 月的中旬。该宣传周旨在激发和宣传网络安全职业意识，推动网络安全职业探索。NCCAW 已经举办了三年，今年将在 2020 年 11 月 9-14 日举办第四届宣传周。回顾过去的 NCCAW 活动，该宣传周的内容重点围绕两个主题展开，一是为什么要从事网络安全职业，二是如何进入网络安全行业。

4．高规格表彰奖励优秀网安人才

美国在 2018 年《国家网络战略》中制定了新的网安人才发展总目标，即“建设更有优势的网络安全人才队伍”，并提出要把“突出和奖励人才”作为一项优先行动计划，对优秀的网络安全教育人员和网络安全专业人员进行奖励和表彰。2019 年 5 月特朗普总统签署《关于美国网络安全人才队伍的行政令》，提出将设立一系列网络安全军功及嘉奖计划，对在网络安全领域做出杰出贡献的军人、文职人员，以及中小学教育者进行表彰。对于联邦政府内的表彰，行政令要求政府各部门应确保在现有的军职和文职人员军功及奖励机制下，网络安全和网络行动领域的杰出表现也能够得到认可，或被授予同等级别的军功及奖励。在必要和适当情况下，各部门应创建新的军功及奖励，对网络安全和网络行动领域中的杰出表现和成就进行表彰。对于联邦政府以外的奖励对象，行政令要求设立“总统网络安全教育奖”，从 2019 年开始每年奖励小学和中学教育者各一人，并重点强调该奖项奖励的是教育者的教育成就，而非其学术研究水平或技术开发能力。到目前为止，“总统网络安全教育奖”已于今

年五月份评选出首批获奖的两名优秀教师。

三、着力加强网安职业意识和专业能力建设

1．进一步营造重视网安人才的环境

理念决定行动。加强网络安全职业意识，提高从业人员的专业能力水平，一方面要严格落实政策法规关于人才建设的合规要求，另一方面也要从根源上提高各单位领导层的网络安全人才意识，营造自上至下重视网安人才、尊重网安专业的环境。关于这一点，习近平总书记在“4·19”网信工作座谈会上明确要求，“各级党委和政府要从心底里尊重知识、尊重人才，为人才发挥聪明才智创造良好条件，营造宽松环境，提供广阔平台”，“要解放思想，慧眼识才，爱才惜才”。建议各级领导干部应积极适应时代要求，强化网络安全思维，真正认识到网络安全人才作为信息时代战略急需资源的重要性，坚持以用为本、急用先行的原则，打造网络安全人才发展的良好环境，让人才的创造活力竞相迸发，聪明才智充分涌流。

2．大力开展信息安全专业人员培训

开展专业培训是提高从业人员整体水平，满足职业化发展需求的重要方法和途径。职业化的一个重要方面，就是要有稳定的知识和能力要求，能够同其他职业进行区分。由于网络安全伴生于各类技术、应用和场景之中，导致网络安全知识和能力的边界难以界定，这给网络安全教育培训带来了极大的挑战。中国信息安全测评中心自 2002 年起推出“注册信息安全专业人员（CISP）”，专门针对安全人员综合能力提升问题，提供系统化的解决方案。经过十余年的发展和完善，CISP 知识体系全面覆盖管理、支撑技术、工程与运营、监管环境等十个知识域，能够有效培养网络安全复合型人才。针对网络安全细分领域众多、技术发展动态性强的特点，CISP 深刻把握网络安全人力资源供给侧结构性改革的内在需求，根据社会的迫

切需要，在网络安全细分方向和前沿领域推出了安全开发、信息系统审计、渗透测试、大数据安全等十余个专业方向，为从业人员深度学习提供更加聚焦的专业培训内容，建立了丰富而全面的网络安全人才培养体系，成为重要行业和关键领域首选的人员资质。

3．加强对网络安全职业和从业者的宣传

加强网络安全职业相关的宣传有助于树立网络安全职业意识，提高全社会对网络安全人才的重视度，促进网络安全人才供需匹配，吸引更多人加入网络安全专业队伍。CISP 作为权威的网络与信息安全专业人员资质，是从业者掌握相应知识和能力、具备业内工作经验和业绩的证明，也是持证人员遵守 CISP 职业道德准则的庄严承诺。在国家党政机关、电力、通信、金融、能源等重要行业的检验下，在各领域网络安全工作者的见证下，CISP 持续输送安全专业人员数万人，成为业内人才评价考核、选拔任用、职业晋阶的必备资质。作为专业网络安全工作者的一张名片，CISP 在自身发展的同时，也为各界提供了了解网安工作任务和进入行业的有效途径。随着专业安全人才缺口不断扩大、安全产业加速发展，对网络安全职业化发展的需求也将日益凸显。未来，CISP 将持续以其全面的知识体系、严格的职业道德准则要求、结合广大持证人员在维护国家网络安全事业中所做的贡献，为树立和强化网络安全职业意识、促进从业者专业能力水平提升提供最准确的诠释和最生动的体现。（来源:《中国信息安全》杂志 2020 年第 9 期）

四、政府之声

➢ 《中华人民共和国个人信息保护法（草案）》发布

2020 年 10 月 21 日，全国人大法工委公开就《中华人民共和国个人信息保护法(草案)》征求意见。以下为关于《中华人民共和国个人信息保护法（草案）》的说明。

一、关于制定本法的必要性

随着信息化与经济社会持续深度融合，网络已成为生产生活的新空间、经济发展的新引擎、交流合作的新纽带。截至 2020 年 3 月，我国互联网用户已达 9 亿，互联网网站超过 400 万个、应用程序数量超过 300 万个，个人信息的收集、使用更为广泛。虽然近年来我国个人信息保护力度不断加大，但在现实生活中，一些企业、机构甚至个人，从商业利益等出发，随意收集、违法获取、过度使用、非法买卖个人信息，利用个人信息侵扰人民群众生活安宁、危害人民群众生命健康和财产安全等问题仍十分突出。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。社会各方面广泛呼吁出台专门的个人信息保护法，本届以来，全国人大代表共有 340 人次提出 39 件相关议案、建议，全国政协委员共提出相关提案 32 件。党中央高度重视网络空间法治建设，对个人信息保护立法工作作出部署。习近平总书记多次强调，要坚持网络安全为人民、网络安全靠人民，保障个人信息安全，维护公民在网络空间的合法权益，对加强个人信息保护工作提出明确要求。为及时回应广大人民群众的呼声和期待，落实党中央部署要求，制定一部个人信息保护方面的专门法律，将广大人民群众的个人信息权益实现好、维护好、发展好，具有重要意义。

第一，制定个人信息保护法是进一步加强个人信息保护法制保障的客观要求。党的十八大以来，全国人大及其常委会在制定关于加强网络信息保护的决定、网络安全法、电子商务法、修改消费者权益保护法等立法工作中，确立了个人信息保护的主要规则；在修改刑法中，完善了惩治侵害个人信息犯罪的法律制度；在编纂民法典中，将个人信息受法律保护作为一项重要民事权利作出规定。我国个人信息保护法律制度逐步建立，但仍难以适应信息化快速发展的现实情况和人民日益增长的美好生活需要。因此，应当在现行法律基础上制定出台专门法律，增强法律规范的系统性、针对性和可操作性，在个人信息保护方面形成更加完备的制度、提供更加有力的法律保障。

第二，制定个人信息保护法是维护网络空间良好生态的现实需要。网络空间是亿万民众共同的家园，必须在法治轨道上运行。违法收集、使用个人信息等行为不仅损害人民群众的切身利益，而且危害交易安全，扰乱市场竞争，破坏网络空间秩序。因此，应当制定出台专门法律，以严密的制度、严格的标准、严厉的责任，规范个人信息处理活动，落实企业、机构等个人信息处理者的法律义务和责任，维护网络空间良好生态。

第三，制定个人信息保护法是促进数字经济健康发展的重要举措。当前，以数据为新生产要素的数字经济蓬勃发展，数据的竞争已成为国际竞争的重要领域，而个人信息数据是大数据的核心和基础。党的十九大报告提出了建设网络强国、数字中国、智慧社会的任务要求。按照这一要求，应当统筹个人信息保护与利用，通过立法建立权责明确、保护有效、利用规范的制度规则，在保障个人信息权益的基础上，促进信息数据依法合理有效利用，推动数字经济持续健康发展。

二、关于起草工作和把握的几点

制定个人信息保护法列入了十三届全国人大常委会立法规划和年度立法工作计划。栗战书委员长和王晨副委员长等常委会领导同志高度重视这项立法工作，多次作出指示批示。2018 年全国人大常委会法制工作委员会会同中央网络安全和信息化委员会办公室，着手研究起草个人信息保护法草案。在起草过程中，认真梳理研究近年来全国人大代表、政协委员提出的建议，召开座谈会听取部分全国人大代表的意见；委托专家组开展专题研究，搜集整理国内外立法资料，形成研究报告；通过多种方式深入调研，广泛征求有关部门、企业和专家等各方面意见。在上述工作的基础上，经反复研究修改，形成了《中华人民共和国个人信息保护法（草案）》。

起草工作注意把握以下几点：一是，坚持立足国情与借鉴国际经验相结合。从我国实际出发，深入总结网络安全法等法律、法规、标准的实施经验，将行之有效的做法和措施上升

为法律规范。从上世纪70年代开始，经济合作与发展组织、亚太经济合作组织和欧盟等先后出台了个人信息保护相关准则、指导原则和法规，有140多个国家和地区制定了个人信息保护方面的法律。草案充分借鉴有关国际组织和国家、地区的有益做法，建立健全适应我国个人信息保护和数字经济发展需要的法律制度。二是，坚持问题导向和立法前瞻性相结合。既立足于个人信息保护领域存在的突出问题和人民群众的重大关切，建立完善可行的制度规范。同时，对一些尚存争议的理论问题，在本法中留下必要空间，对新技术新应用带来的新问题，在充分研究论证的基础上作出必要规定，体现法律的包容性、前瞻性。三是，处理好与有关法律的关系。把握权益保护的立法定位，与民法典等有关法律规定相衔接，细化、充实个人信息保护制度规则。同时，与网络安全法和已提请全国人大常委会审议的数据安全法草案相衔接，对于网络安全法、数据安全法草案确立的网络和数据安全监管相关制度措施，本法不再作规定。

三、关于草案的主要内容

草案共八章七十条，主要内容包括：

（一）明确本法适用范围

一是，对本法相关用语作出界定，规定：个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息；个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开等活动。（草案第四条）

二是，明确在我国境内处理个人信息的活动适用本法的同时，借鉴有关国家和地区的做法，赋予本法必要的域外适用效力，以充分保护我国境内个人的权益，规定：以向境内自然人提供产品或者服务为目的，或者为分析、评估境内自然人的行为等发生在我国境外的个人信息处理活动，也适用本法；并要求境外的个人信息处理者在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。（草案第三条、第五十二条）

（二）健全个人信息处理规则

一是，确立个人信息处理应遵循的原则，强调处理个人信息应当采用合法、正当的方式，具有明确、合理的目的，限于实现处理目的的最小范围，公开处理规则，保证信息准确，采取安全保护措施等，并将上述原则贯穿于个人信息处理的全过程、各环节。（草案第五条至第九条）

二是，确立以“告知—同意”为核心的个人信息处理一系列规则，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，并且个人有权撤回同意；重要事项发生变更的应当重新取得个人同意；不得以个人不同意为由拒绝提供产品或者服务。考虑到经济社会生活

的复杂性和个人信息处理的不同情况，草案还对基于个人同意以外合法处理个人信息的情形作了规定。（草案第十三条至第十九条）

三是，根据个人信息处理的不同环节、不同个人信息种类，对个人信息的共同处理、委托处理、向第三方提供、公开、用于自动化决策、处理已公开的个人信息等提出有针对性的要求。（草案第二十一条至第二十八条）

四是，设专节对处理敏感个人信息作出更严格的限制，只有在具有特定的目的和充分的必要性的情形下，方可处理敏感个人信息，并且应当取得个人的单独同意或者书面同意。（草案第二十九条至第三十二条）

五是，设专节规定国家机关处理个人信息的规则，在保障国家机关依法履行职责的同时，要求国家机关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。（草案第三十三条至第三十七条）

在应对新冠肺炎疫情中，大数据应用为联防联控和复工复产提供了有力支持。为此，草案将应对突发公共卫生事件，或者紧急情况下保护自然人的生命健康，作为处理个人信息的合法情形之一。需要强调的是，在上述情形下处理个人信息，也必须严格遵守本法规定的处理规则，履行个人信息保护义务。

（三）完善个人信息跨境提供规则

一是，明确关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的处理者，确需向境外提供个人信息的，应当通过国家网信部门组织的安全评估；对于其他需要跨境提供个人信息的，规定了经专业机构认证等途径。（草案第三十八条、第四十条）

二是，对跨境提供个人信息的“告知—同意”作出更严格的要求。（草案第三十九条）

三是，对因国际司法协助或者行政执法协助，需要向境外提供个人信息的，要求依法申请有关主管部门批准。（草案第四十一条）

四是，对从事损害我国公民个人信息权益等活动的境外组织、个人，以及在个人信息保护方面对我国采取不合理措施的国家和地区，规定了可以采取的相应措施。（草案第四十二条、第四十三条）

（四）明确个人信息处理活动中个人的权利和处理者义务

一是，与民法典的有关规定相衔接，明确在个人信息处理活动中个人的各项权利，包括知情权、决定权、查询权、更正权、删除权等，并要求个人信息处理者建立个人行使权利的申请受理和处理机制。（草案第四十四条至第四十九条）

二是，明确个人信息处理者的合规管理和保障个人信息安全等义务，要求其按照规定制

定内部管理制度和操作规程，采取相应的安全技术措施，并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、向境外提供个人信息等高风险处理活动，事前进行风险评估；履行个人信息泄露通知和补救义务等。（草案第五十条、第五十一条、第五十三条至第五十五条）

（五）关于履行个人信息保护职责的部门

个人信息保护涉及各个领域和多个部门的职责。草案根据个人信息保护工作实际，明确国家网信部门负责个人信息保护工作的统筹协调，发挥其统筹协调作用；同时规定：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。（草案第五十六条）此外，草案还对违反本法规定行为的处罚及侵害个人信息权益的民事赔偿等作了规定。（来源：中国人大网）

- **《中华人民共和国个人信息保护法（草案）》全文：**
- http://www.npc.gov.cn/flcaw/flca/ff80808175265dd401754405c03f154c/attachment.pdf

➢ 十四部门印发 《2020 网络市场监管专项行动（网剑行动）方案的通知》

2020 年 10 月 24 日，为深入贯彻落实党中央和国务院有关决策部署，充分发挥网络市场监管部际联席会议各成员单位职能优势，继续推进《电子商务法》贯彻落实，着力规范网络市场经营秩序，网络市场监管部际联席会议成员单位联合印发通知，组织开展 2020 网络市场监管专项行动（网剑行动）。

一、《通知》印发背景

2016 年 12 月，国务院办公厅函复原工商总局同意建立网络市场监管部际联席会议制度。联席会议成员单位由原工商总局、发展改革委等 10 个部门组成，原工商总局为牵头单位。2020 年 7 月，国务院办公厅函复同意调整完善网络市场监管联席会议制度。调整完善后的联席会议成员单位由市场监管总局、中央宣传部、工业和信息化部、公安部、商务部、文化和旅游部、人民银行、海关总署、税务总局、网信办、林草局、邮政局、药监局、知识产权局等 14 个单位组成，市场监管总局为牵头单位。从 2017 年开始，联席会议成员单位每年联合开展网剑行动，加强协同联动，着力规范网络市场经营秩序。2020 网络市场监管专项行动（网剑行动）是联席会议制度调整完善后首次开展的专项行动。

二、《通知》制定依据

以落实《电子商务法》为统领，按照《国务院办公厅关于促进平台经济规范健康发展的指导意见》相关要求，依据《电子商务法》《消费者权益保护法》《反垄断法》《反不正当竞争法》《合同法》《价格法》《网络安全法》等法律法规，规范网络市场竞争秩序。

三、《通知》主要内容

按照通知要求，2020 网络市场监管专项行动（网剑行动）将围绕七项重点任务开展：一是落实电商平台责任，夯实监管基础。按照《电子商务法》等法律法规要求，依法督促电子商务平台落实平台责任；规范电子商务经营主体，集中整治非法主体互联网应用。二是重拳打击不正当竞争行为，规范网络市场竞争秩序。按照《反垄断法》《反不正当竞争法》《电子商务法》等法律规定，严厉打击排除、限制竞争及妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行行为，依法查处电子商务平台经营者对平台内经营者进行不合理限制或者附加不合理条件等行为。三是集中治理网上销售侵权假冒伪劣商品，守住安全底线。以食品（含保健食品）、药品、医疗器械、防疫用品、化妆品、儿童用品、服装鞋帽、家居家装、汽车及配件等舆情热点、社会反映集中、关系公众生命健康安全的产品为重点，开展集中整治，强化线上线下联合监管和信息共享，严惩违法犯罪行为。四是严厉打击野生动植物及其制品非法交易行为，保护野生动植物资源和公共卫生安全。严肃查处通过微博、微信、视频网站、直播平台等网络社交平台，发布、直播和恶意传播、转发违法猎捕、杀害、吃食、加工、虐待和利用野生动物及制品的视频和网络直播行为；加大野生动植物及其制品交易监管力度，全面禁止网上非法野生动植物交易。五是强化互联网广告监管，维护互联网广告市场秩序。集中整治社会影响大、覆盖面广的门户网站、搜索引擎、电子商务平台、移动客户端

和新媒体账户等互联网媒介上发布违法广告行为，曝光一批大案要案。六是依法整治社会热点问题，营造良好网络市场环境。规范“直播带货”等网络经营活动秩序，依法惩处“直播带货”等领域违法犯罪行为；加强二手物品网络交易平台监管，依法打击借众筹名义实施非法集资、诈骗等违法犯罪行为，依法整治社会热点问题。七是依法查处其他网络交易违法行为，保护消费者合法权益。

下一步，市场监管总局等部门将充分发挥网络市场监管联席会议作用，加强工作督促指导，积极推动专项行动各项工作稳步推进，不断净化网络市场环境，保护消费者和经营者合法权益，促进网络经济健康发展。（来源：国家市场监督管理总局）

➢ 《中华人民共和国未成年人保护法修订》2021 年 6 月 1 日施行

2020 年 10 月 17 日，十三届全国人大常委会第二十二次会议表决通过修订后的《未成年人保护法》，增设“网络保护”专章，对近年来社会各界高度关注的未成年人网络保护问题作出专门规定，并将于 2021 年 6 月 1 日正式施行。

此次法律修订立足当前未成年人网络保护实际，顺应数字时代互联网发展趋势和规律，为我国未成年人网络保护工作提供了坚实的法律保障，也推动未成年人网络保护法治建设进入新的发展阶段。 **网络保护突出十大制度亮点：**《未成年人保护法》“网络保护”专章共计十七条，此外总则、社会保护、司法保护章节中也有相关条款，涵盖了未成年人网络保护的诸多方面，总结来看主要包括以下十大制度。

一是完善了未成年人网络保护监管体制。二是依法保护未成年人网络权益和上网安全。

三是明确规定未成年人网络素养培育和提升。四是高度重视未成年人沉迷网络预防和干预。五是创设可能影响未成年人身心健康信息提示管理制度。六是要求预装上网保护软件并作出选择性规定。七是进一步强化未成年人个人信息保护。八是对未成年人易于沉迷的内容进行重点监管。九是针对网络欺凌问题作出专门规定。十是建立未成年人网络保护投诉举报机制。（来源：网信中国）

- **《中华人民共和国未成年人保护法》全文：**
- http://www.npc.gov.cn/npc/c30834/202010/82a8f1b84350432cac03b1e382ee1744.shtml

➢ 《互联网用户公众账号信息服务管理规定（修订草案征求意见稿）》发布

2020 年 10 月 15 日，国家互联网信息办公室发布《互联网用户公众账号信息服务管理规定（修订草案征求意见稿）》，公开征求意见。

意见提出，公众账号信息服务平台应当依法依约禁止公众账号生产运营者违规转让借用或者非法交易买卖公众账号。公众账号生产运营者向其他用户转让或赠与公众账号使用权的，应当向平台提出申请。平台应当依据前款规定对受让方用户进行认证核验，并公示主体变更信息。平台发现生产运营者未经审核擅自转让公众账号的，应当及时暂停或终止提供服务。（来源：国家互联网信息办公室）

- **《互联网用户公众账号信息服务管理规定（修订草案征求意见稿）》**
- **全文：**http://www.cac.gov.cn/2020-10/15/c_1604325530663495.htm

五、本期重要漏洞实例

➢ Microsoft 发布 2020 年 10 月安全更新

发布日期：2020-10-13

更新日期：2020-10-13

描述：2020 年 10 月 13 日，微软发布了 2020 年 10 月份的月度例行安全公告，修复了其多款产品存在的 87 个安全漏洞。受影响的产品包括：Windows 10 2004 & WindowsServer v2004（51 个）、Windows 10 1909 & WindowsServer v1909（50 个）、Windows 10 1903 & WindowsServer v1903（50 个）、Windows 8.1 & Server 2012 R2（20 个）、Windows RT 8.1（18 个）、Windows Server 2012（18 个）和 Microsoft Office-related software（21 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	公告标题和摘要	最高严重等级和漏洞影响	受影响的软件
CVE-2020-16898	**Windows TCP/IP 远程执行代码漏洞** Windows TCP/IP 堆栈未能正确地处理 ICMPv6 路由器播发数据包时，存在一个远程执行代码漏洞。成功利用此漏洞的攻击者可以获得在目标服务器或客户端上执行代码的能力。 要利用此漏洞，攻击者必须将特制的 ICMPv6 路由器广告数据包发送到远程 Windows 计算机。 此更新通过更正 Windows TCP/IP 堆栈处理 ICMPv6 路由器播发数据包的方式来解决此漏洞。	严重 远程代码执行	Windows 10 Server 2019 Server, version 1903 Server, version 1909 Server, version 2004
CVE-2020-16885	**Windows Storage VSP Driver 特权提升漏洞** Windows Storage VSP Driver 不适当地处理文件操作时，存在特权提升漏洞。成功利用此漏洞的攻击者可以获得更高的特权。 要利用此漏洞，攻击者首先需要在受害者系统上执行代码。然后，攻击者可以运行特制的应用程序。 该安全更新通过确保 Windows Storage VSP Driver 正确处理文件操作来解决此漏洞。	重要 特权提升	Windows 10 Server 2016 Server 2019 Server, version 1903 Server, version 2004
CVE-2020-16908	**Windows 安装程序特权提升漏洞** Windows 安装程序以处理目录的方式存在一个特权提升漏洞。本地身份验证的攻击者可以以提升的系统特权运行任意代码。成功利用此漏洞后，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。 该安全更新通过确保 Windows 安装程序正确处理目录来解决此漏洞。	重要 特权提升	Windows 10
CVE-2020-16909	**Windows Error Reporting 特权提升漏洞**	重要 特权提升	Windows 10 Server 2016

	WER 处理和执行文件时，Windows Error Reporting（WER）中存在一个特权提升漏洞。 如果攻击者可以成功利用此漏洞，则可以允许特权提升。 成功利用此漏洞的攻击者可以获得对敏感信息和系统功能的更大访问权限。要利用此漏洞，攻击者可以运行特制应用程序。 该安全更新通过更正 WER 处理和执行文件的方式来解决漏洞。		Server 2019 Server, version 1903 Server, version 1909 Server, version 2004
CVE-2020-16891	**Windows Hyper-V 远程执行代码漏洞** 当主机服务器上的 Windows Hyper-V 未能正确验证来宾操作系统上经过身份验证的用户输入时，将存在一个远程执行代码漏洞。要利用此漏洞，攻击者可以在客户机操作系统上运行特制的应用程序，会导致 Hyper-V 主机操作系统执行任意代码。 成功利用此漏洞的攻击者可以在主机操作系统上执行任意代码。 该安全更新通过更正 Hyper-V 验证访客操作系统用户输入的方式来解决此漏洞。	严重 远程代码执行	Windows 10 Server 2016 Server 2019 Server, version 1903 Server, version 1909 Server, version 2004 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-16911	**GDI +远程代码执行漏洞** Windows Graphics Device Interface（GDI）处理内存中的对象方式存在一个远程执行代码漏洞。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。与使用管理用户权限进行操作的用户相比，将其帐户配置为在系统上具有较少用户权限的用户受到的影响较小。 该安全更新通过更正 Windows GDI 处理内存中对象的方式来解决漏洞。	严重 远程代码执行	Windows 10 Server 2016 Server 2019 Server, version 1903 Server, version 1909 Server, version 2004 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-16947	**Microsoft Outlook 远程执行代码漏洞** 当该软件未能正确处理内存中的对象时，Microsoft Outlook 软件中将存在一个远程执行代码漏洞。成功利用此漏洞的攻击者可以在系统用户的上下文中运行任意代码。如果当前用户使用管理用户权限登录，则攻击者可以控制受影响的系统。然后，攻击者可以安装程序。查看，更改或删除数据；或创建具有完全用户权限的新帐户。与使用管理用户权限进行操作的用户相比，将其帐户配置为在系统上具有较少用户权限的用户受到的影响较小。 该安全更新通过更正 Outlook 处理内存中对象的方式来解决此漏洞。	严重 远程代码执行	Office 2019 365 Apps Enterprise Outlook 2016
CVE-2020-16929	**Microsoft Excel 远程执行代码漏洞** 当该软件未能正确处理内存中的对象时，Microsoft Excel 软件中将存在一个远程执行代码漏洞。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	重要 远程代码执行	Office 2010/2013/2016/2019 365 Apps Enterprise Excel 2010/2013/2016

	意代码。如果当前用户使用管理用户权限登录，则攻击者可以控制受影响的系统。然后，攻击者可以安装程序。查看，更改或删除数据；或创建具有完全用户权限的新帐户。与使用管理用户权限进行操作的用户相比，将其帐户配置为在系统上具有较少用户权限的用户受到的影响较小。 该安全更新通过更正 Microsoft Excel 处理内存中对象的方式来解决此漏洞。		SharePoint Server 2010 SharePoint Enterprise Server 2013 Excel Web App 2010 Office Web Apps 2010/2013 Office Online Server Office 2016/2019 for Mac
CVE-2020-16951	**Microsoft SharePoint 远程执行代码漏洞** 当软件未能检查应用程序包的源标记时，Microsoft SharePoint 存在一个远程执行代码漏洞。成功利用此漏洞的攻击者可以在 SharePoint 应用程序池和 SharePoint 服务器场帐户的上下文中运行任意代码。要利用此漏洞，需要用户将特制的 SharePoint 应用程序包上载到受影响的 SharePoint 版本。 该安全更新通过更正 SharePoint 如何检查应用程序包的源标记的方式来解决漏洞。	严重 远程代码执行	SharePoint Foundation 2013 SharePoint Enterprise Server 2016 SharePoint Server 2019

参考链接：
https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Oct

➢ Linux kernel 内存破坏和读取溢出漏洞

发布日期：2020-10-16
更新日期：2020-10-16
受影响系统：
Linux kernel 5.9-rc7
描述：

CVE(CAN) ID: CVE-2020-25643
Linux kernel 是一种计算机操作系统内核，以 C 语言和汇编语言写成，符合 POSIX 标准，按 GNU 通用公共许可证发行。Linux kernel 5.9-rc7 之前版本中的 HDLC_PPP 模块存在内存破坏和读取溢出漏洞。该漏洞源于 ppp_cp_parse_cr 函数的输入验证不当。攻击者可利用该漏洞导致系统崩溃。
建议：

厂商补丁：

Linux
厂商已发布了漏洞修复程序，请及时关注更新：
https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/commit/?id=66d42ed8b25b64eb63111a2b8582c5afc8bf1105

➢ Cisco IOS XE 任意代码执行漏洞

发布日期：2020-10-15
更新日期：2020-10-15
受影响系统：Cisco IOS XE
描述：

CVE(CAN) ID: CVE-2020-3423
Cisco IOS XE 是美国 Cisco 公司为其网络设备开发的一套基于 Linux 内核的模块化操作系统。Cisco IOS XE 中 Lua 解释器的实现存在任意代码执行漏洞。该漏洞源于在用户提供的 Lua 脚本的上下文中对 Lua 函数调用的限制不足。攻击者可通过提交恶意 Lua 脚本利用该漏洞在受影响的设备的底层 Linux OS 上以 root 权限执行任意代码。
建议：

厂商补丁：
Cisco
厂商已发布了漏洞修复程序，请及时关注更新：
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-lua-rce-7VeJX4f

➢ Gitlab runner 命令注入漏洞

发布日期：2020-10-15
更新日期：2020-10-15
受影响系统：
GitLab GitLab runner <13.2.4
GitLab GitLab runner 13.3.2
GitLab GitLab runner 13.4.1
描述：

CVE(CAN) ID: CVE-2020-13347
GitLab 是美国 GitLab 公司的一款使用 Ruby on Rails 开发的、自托管的、Git（版本控制系统）项目仓库应用程序。该程序可用于查阅项目的文件内容、提交历史、Bug 列表等。Gitlab runner 13.2.4 之前版本,13.3.2 版本，13.4.1 版本存在安全漏洞，该漏洞源于在 Windows 系统上 docker executor,攻击者可利用该漏洞在 Windows 主机上运行任意命令,通过 DOCKER_AUTH_CONFIG 构建变量。
建议：

厂商补丁：
GitLab
目前厂商暂未发布修复措施解决此安全问题，建议用户随时关注厂商主页或参考网址以获取解决办法：
https://hackerone.com/users/sign_in

六、本期网络安全事件

➢ 全球交易所遭遇水逆月 接二连三发生宕机故障

2020 年 10 月 22 日报道，本月，市场遭遇三连击，三大洲的交易所接连宕机：先是东京证交所，然后是墨西哥证交所，最后是泛欧交易所。在巴黎上市的泛欧交易所一旦完成以 50 亿美元收购意大利证交所的交易，将处理全欧洲 25%的股票交易。但在周一（19 日）早上，交易中断了三个小时，是这家交易所运营商两年来遭遇的最严重交易中断。

泛欧交易所

尽管宕机通常是由软件故障、硬件问题或网络攻击引起的，但泛欧交易所表示此次宕机是因为“中间件系统”问题。巴黎、布鲁塞尔、阿姆斯特丹、里斯本和都柏林的交易均因此中断。“打个比方，飞行员过去用的是仪表板和一个控制方向舵的操纵杆，但现在中间有个环节，操纵杆发送指令给电脑，然后电脑去操作方向舵，”Market Structure Partners 创始人 Niki Beattie 说。“当中间件出现问题时，就好像操纵杆失灵了。”泛欧交易所 2018 年升级到一个名为 Optiq 的专有平台，该公司在其网站声称该平台具有“高度可靠性”，并满足“减少事故的监管要求”。泛欧交易所拒绝透露在该平台上花了多少钱。彭博汇总的数据显示，该公司过去 10 年 4.6%的自由现金流用于资本支出，相当于 8，120 万美元。墨西哥证交所花了约 2.3%，相当于 1，600 万美元。

东京和墨西哥

日本的交易所故障发生在 10 月 1 日。问题出在一个名为 Device 1 的共享磁盘设备中，构成东京证交所 Arrowhead 交易系统的各个服务器都使用该磁盘存储的数据。它负责为监控交易的终端分配信息，例如指令、用户名/密码组合等。设备内存组件故障导致错误，这个错误本应触发故障切换——自动切换到备份。但由于系统与其手册之间的差异导致一个设置错误（自 2015 年以来一直潜藏），故障切换并未启动。日本金融厅计划对东证进行调查，并可能要求采取行政措施。

在墨西哥，因未获授权谈论此事而要求不具名的现任和前任交易所官员均表示，墨西哥证交所遭遇近些年最长宕机停摆，所有系统冗余都未能奏效。

墨西哥证交所表示，10 月 9 日（周五）。长达 10 小时的交易暂停是由于技术提供商的一个错误。该交易所否认了遭遇网络攻击的谣言，但未提供更多细节。证交所一位官员告诉彭博新闻社，交易所数据中心提供商 Kio Networks 的主服务器出现问题，导致宕机。Kio 的发言人拒绝置评。交易暂停之后，墨西哥证交所也无法启动其备用系统，而该备用系统此前已经通过当地监管机构的测试。知情人士说，这让备用系统的可靠性和监管机构检查的有效性都令人生疑。监管机构 CNBV 没有回应置评请求。（来源：新浪）

➢ 黑客控制服务器 103 台，被判 3 年缓刑 4 年罚金 15000

2020 年 10 月 12 日报道，“90 后”男子小陶通过网络专业工具将“菜刀”软件中的获取地址修改成自己的收取地址，再将地址上传至国内知名中文 IT 技术交流网站及多个 QQ 群内对外发布，利用他人下载使用软件的契机非法获取了 1 万余条网站后门漏洞信息，随后通过租赁上述信息非法获利人民币 1.1 万元。近日，邗江法院开庭审理了此案。

一、小伙悟出赚钱偏门，网络世界中寻觅商机

小陶是福建省南平市当地人，专科毕业后就赋闲在家。一直没能找到合适工作的小陶手头拮据，赚钱成了他的头等大事。因为平日里操作计算机较熟练，再加上掌握一些编程知识技能，小陶将目光投向了黑客网络技术领域。

2019 年 2 月，小陶察觉网络黑客生意利润丰厚且有市场前景。出于赚钱的目的，他先在网站上下载名为“菜刀”的黑客软件，然后用“易语言”软件对“菜刀”软件的下载地址进行修改，改成自己的地址。随后再将修改过的网址上传至国内某知名的专业 IT 技术交流

平台网站以及他日常管理的四个 QQ 群内供他人免费下载。

用户下载并使用被小陶修改过的“菜刀”软件时，收集来的网站后门信息就会自动回传到小陶的网络硬盘内。这些步骤逐一完成后，小陶就悄悄拥有了这些网站的实际控制权限。一番操作后，小陶便能利用非正规手段入侵这些网站，顺利控制网站数据。小陶将收集来的大量网站后门信息在网上销售给需要的人，从中牟取利润。

二、警方火眼金睛，揪出网络“黑客”

小陶的发财梦没有持续多久，扬州警方经过缜密侦查，收集掌握其大量违法犯罪证据。去年 4 月中旬，市公安局网安支队民警在工作中发现，有网民登录某网址管理后台并进行编辑维护，且该网站中存在 8000 多个网站漏洞。经测试发现，网站中的部分存活状态漏洞可直连被入侵互联网服务器获取控制权。在随后的侦查过程中，警方经落地查证发现，福建籍男子小陶有重大作案嫌疑。去年 7 月 10 日，扬州警方在福建省南平市将犯罪嫌疑人小陶抓获，到案后小陶对其犯罪事实供认不讳。

三、“黑客”非法控制，计算机信息系统被判刑

近日，经邗江检察院提起公诉，邗江法院对这起案件进行公开开庭审理。法院经审理查明，2019 年 2 月至 7 月，被告人小陶在福建省南平市家中，将事先修改过回收地址的“菜刀”软件通过上传至某网站以及在其管理的 QQ 群内对外发布，利用他人下载使用该软件时

非法获取了 1 万余条网站后门漏洞信息，后通过租赁上诉信息非法获利人民币 1.1 万元。经远程勘验 1 万余条网站漏洞信息中可直连被入侵互联网服务器获取控制权限的达 103 台。

法院认为，被告人小陶违反国家规定，对国家事务、国防建设、尖端科学以外的计算机信息系统实施非法控制，情节特别严重，其行为已构成非法控制计算机信息系统罪。依据《中华人民共和国刑法》等法律，法院最终判决，被告人小陶犯非法控制计算机信息系统罪，判处有期徒刑三年，缓刑四年，并处罚金人民币一万五千元。（来源：扬州晚报）

➢ 希腊电信公司遭黑客攻击 数百万个电话数据被窃取

2020 年 10 月 16 日，据欧联网援引欧联通讯社报道，希腊最大电信公司 Cosmote15 日向媒体通报，该公司上个月发生了一起重大的数据泄露事件，数以百万计希腊民众的电话以及信息数据被窃取，其中甚至包括总理和政府高级官员的通信数据。

据报道，此前，Cosmote 公司数据库遭到不明身份黑客的网络攻击。黑客窃取了 2020 年 9 月 1 日至 5 日期间的数百万个电话和短信的资料，包括固定电话、移动电话、移动网络等。

根据 Cosmote 发布的公告显示，该公司在对其系统进行检查时，发现有一个未经授权的操作，从公司大数据系统中导出带有呼叫详细信息的文件。数据中包含电话号码、通话日期和时间、基站坐标等。但这些文件中不包含通话和聊天信息内容、用户姓名和地址、密码、信用卡或银行帐户信息等个人资料。

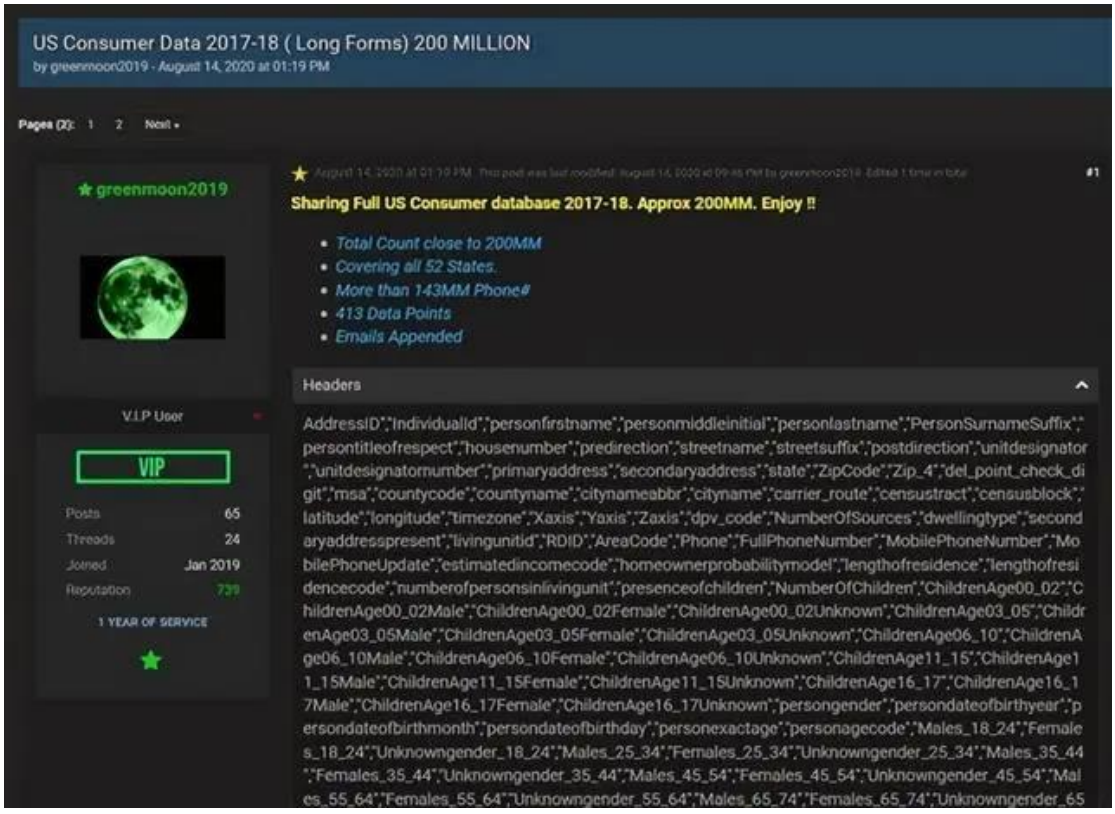
Cosmote 管理层高度重视此次事件，称黑客来自国外。该公司称，希望该行动仅出于商

业目的，而不涉及国家安全问题。Cosmote 还称，事后已经立即封锁通道，并采取一切必要的保护措施，第一时间通知了主管部门，客户无需采取任何行动。据悉，该事件正在调查中。到目前为止，没有迹象表明被非法窃取的资料被公开或以其它方式使用。（来源：中国新闻网）

➢ 美国 1.86 亿选民数据在暗网被黑客出售，FBI 介入调查

2020 年 10 月 22 日，据 NBC 新闻网报道，美国一家网络安全公司 Trustwave 表示，他们发现一名黑客正在出售超过 2 亿美国人的个人识别信息，其中包括 1.86 亿选民的注册数据。

网络安全公司 Trustwave 表示，他们识别出的大部分数据都是公开可用的，并且几乎所有数据都是可供合法企业定期买卖的。但事实上，他们发现大量有关姓名、电子邮件地址、电话号码和选民登记记录的信息数据在暗网成批出售。



“如此大量的美国公民数据可能会被用作网络犯罪，或被国外的对手利用。”Trustwave 公司的副总裁，负责安全研究领域的齐夫·马多尔说道。据称，他正是发现这些公民数据的人。他补充说：“在大选之前、之中和之后，不法分子很容易就能用这些选民和消费者数据宣传虚假信息，通过社交媒体、电子邮件、网络钓鱼以及电话诈骗实施不法活动。”他表示，

近年来黑客对大量公司进行网络攻击，窃取了公民信息，并从政府网站上抓取公开数据，这些数据构成了泄露在暗网上的信息数据。据悉，在美国大多数州，选民登记信息是向外公开的。

报道称，Trustwave 公司一直监视着暗网论坛，寻找对安全构成威胁的信息，期间遇到了一个自称为“Greenmoon2019”的黑客，该黑客提出要出售数据。工作人员使用虚拟身份诱使黑客提供更多信息，其中包括该黑客用来收款的比特币钱包。

暗网上的比特币钱包会公开显示交易信息，但不显示交易者的身份。马多尔说，他们追踪到这名黑客在 5 月份创建的另一个有着巨额收入的比特币钱包，钱包内含有 1 亿美元的资金。他们分析后认为，这些钱是这名黑客的非法收益，不过并非所有非法资金都来自于销售数据的收入。

个人信息泄露并不是什么新鲜事，但是随着美国大选的临近，如此巨大的数据泄露意味着不法分子可以轻松破坏选举。Trustwave 方面称，黑客共提供了 1.86 亿个选民数据和 2.45 亿个其他个人数据记录。

选民登记数据在许多州都是公开的，但选民的电子邮件地址通常不会公开。马多尔说，这名黑客利用他窃取的其他数据，将公民的电子邮件地址与选民名册配对，将其打包出售。此外，通过利用这名黑客出售的数据，不法分子还能将攻击目标锁定为仅支持民主党或共和党的选民，并提供了他们的电子邮件地址。目前，Trustwave 公司表示，他们已将其收集的资料移交给了 FBI，FBI 正在对此进行调查。（来源：NBC 新闻网）

➢ 六家银行因侵害个人信息被罚逾 4000 万元

2020 年 10 月 21 日，央行公告显示，近日，央行相关分支机构依法对部分金融机构侵害消费者金融信息安全行为立案调查，分别对农业银行吉林市江北支行、中国银行石嘴山市分行、建设银行德阳分行、建设银行娄底分行、建设银行东营分行、建设银行建德支行及相关责任人予以警告并处以罚款。

央行同日公布的罚单显示，农行、中行、建行 3 家银行共 6 家分支行被罚超 4000 万。其中，农行吉林市江北支行的处罚理由为侵害消费者个人信息依法得到保护的权利和违反反洗钱管理规定、泄露客户信息，受警告及 1223 万元罚款处罚，相关责任人罚款从 1.75 万元到 3 万元不等。另外，建行德阳分行被罚 1406 万元，也是此轮处罚公示中的最高处罚金额。

行政处罚信息公示表

行政相对人名称	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
中国农业银行股份有限公司吉林市江北支行	吉市银罚字〔2020〕2 号	1. 侵害消费者个人信息依法得到保护的权利； 2.违反反洗钱管理规定，泄露客户信息。	警告，并处 1223 万元罚款	中国人民银行吉林市中心支行	2020 年 10 月 20 日
丁浩洋（时任中国农业银行股份有限公司吉林市江北支行营业室员工）	吉市银罚字〔2020〕3 号	对违反反洗钱管理规定，泄露客户信息违法违规行为负有直接责任。	罚款 3 万元	中国人民银行吉林市中心支行	2020 年 10 月 20 日
葛振东（时任中国农业银行股份有限公司吉林市江北支行行长）	吉市银罚字〔2020〕4 号	对违反反洗钱管理规定，泄露客户信息违法违规行为负有责任。	罚款 1.75 万元	中国人民银行吉林市中心支行	2020 年 10 月 20 日
金宇峰（时任中国农业银行股份有限公司吉林市江北支行副行长）	吉市银罚字〔2020〕5 号	对违反反洗钱管理规定，泄露客户信息违法违规行为负有责任。	罚款 1.75 万元	中国人民银行吉林市中心支行	2020 年 10 月 20 日
白松灵（时任中国农业银行股份有限公司吉林市江北支行营业室业务主管）	吉市银罚字〔2020〕6 号	对违反反洗钱管理规定，泄露客户信息违法违规行为负有责任。	罚款 1.75 万元	中国人民银行吉林市中心支行	2020 年 10 月 20 日

央行相关负责人表示，前期，部分媒体报道了个别金融机构员工涉嫌泄露消费者金融信息。人民银行依据属地原则调查立案，发现涉案金融机构存在侵害消费者金融信息安全权的行为，依法依规对涉案金融机构严肃查处。

央行在依法作出行政处罚的同时，责令涉案金融机构以此为戒，全面排查消费者金融信息保护安全隐患，及时进行整改。一是在制度建设层面，明确要求其进一步健全完善消费者金融信息收集、保存、使用、对外提供等环节的内控制度，采取有效措施将各项制度落到实处。二是在系统建设方面，金融机构要持续改进完善业务系统和反洗钱系统，建立用户异常行为监测模型，定期监测并堵塞系统存在的技术漏洞等安全隐患;完善系统功能模块，确保系统生成日志能及时、准确、全面地记录信息数据的查询和下载操作。特别是要畅通系统使用人员的意见反馈渠道，避免业务、技术“两层皮”的现象。三是在人员管理方面，要不断强化相关措施。对接触消费者金融信息的岗位人员合理设置权限，并采取内部审批等有效措施进行权限控制，全面开展员工业务培训和警示教育工作，有效避免泄露消费者金融信息行为的再次发生。

下一步，央行将进一步强化消费者金融信息安全监管和反洗钱信息保密工作，督促金融机构履行主体责任，持续完善有利于保护消费者金融信息安全和落实《反洗钱法》信息保密要求在内的各项金融消费者权益机制，切实保护金融消费者长远和根本利益。

此外，央行相关负责人提醒，金融消费者保护自己的金融信息安全，重点要把握好以下几方面：要保管好身份证件、银行卡、银行(支付)账户等，不要转借他人使用;切勿向他人透露个人金融信息、财产状况等基本信息，不要随意在各类线上线下渠道留下个人金融信息;尽量亲自办理金融业务，切勿委托不熟悉的人或中介代办;提供个人身份证件复印件办理各类业务时，要在复印件上注明使用用途;不要随意丢弃刷卡签购单、取款凭条、信用卡对账单等;不要轻易点击来历不明的手机短信、邮件和不明链接，不要随意扫描来历不明的二维码，谨慎使用公共 WIFI、免密 WIFI;发现个人金融信息泄露风险，要及时联系公安等部门维权。（来源：中国人民银行）

➢ 英国航空因数据泄露的巨额罚款 减至 2000 万英镑

2020 年 10 月 16 日，据英国天空新闻台报道，英国数据安全监管部门信息专员办公室对英国航空公司因 2018 年客户数据泄露事件罚款 2000 万英镑，约合人民币 1.7 亿元。而去年通知该公司的罚款金额为 1.83 亿英镑。根据信息专员办公室的说法，在确定最终罚款之前，考虑到新冠肺炎疫情对英航业务的影响，因此办公室做此决定。据了解，尽管减少了 1.63 亿英镑的罚款，这笔罚金仍是有史以来最高的。

2018 年 9 月，英航披露公司数据遭窃，大约 38 万笔交易受到影响，超过 40 万名客户的信息被泄露。

ICO 在历时近两年的调查后得出了结论：英国航空公司没有落实到位的安全措施来处理大量的个人数据。这家监管机构表示，这次事件违反了数据保护法。据悉，攻击者已访问了英国航空公司 24.4 万客户的姓名、地址、支付卡号和信用卡验证值(CVV)号。另有 77000 个客户的支付卡号和 CVV 号被访问，另外 108000 个客户只是卡号被访问。该监管机构表示，英国航空公司行政俱乐部多达 612 名成员的用户名和密码也可能已经被访问。

英国航空公司在两个多月后才意识到数据已泄露。

信息专员 Elizabeth Denham 在一份声明中说：“人们将他们的个人资料托付给英国航空公司，英国航空公司却没有采取到位的措施来确保这些资料的安全。”“它未能采取行动是不可接受的，影响了成千上万的人，因而可能给他们造成一些焦虑和困扰。这就是为什么我们对英国航空公司开出 2000 万英镑的罚单，这是我们迄今最高的一笔罚单。”

“如果组织对人们的个人数据做出糟糕的决定，这可能会对人们的生活产生重大的影响。现在法律为我们提供了工具，鼓励企业对于数据做出更合理的决策，包括购置最新的安全解决方案。”

英国航空公司的发言人告诉 CNBC：“我们在 2018 年一意识到我们的系统遭到犯罪分子的攻击，便立即通知了客户;很遗憾，我们并没有达到客户的期望。”“我们很高兴 ICO 认识到自那次攻击以来我们已经在系统安全方面做出了很大的改进，我们完全配合其调查工作。”（来源：安全学习那些事）

信息安全意识产品服务

021-33663299