国家网络安全宣传周
China Cybersecurity Week

网络安全为人民
网络安全靠人民

9TH

9月5日-9月11日

2022年陕西省第九届
国家网络安全宣传周

THE NINTH NATIONAL CYBER SECURITY PUBLICITY WEEK OF SHAANXI PROVINCE

2022年
国家网络安全宣传周
NETWORK SECURITY PUBLICITY

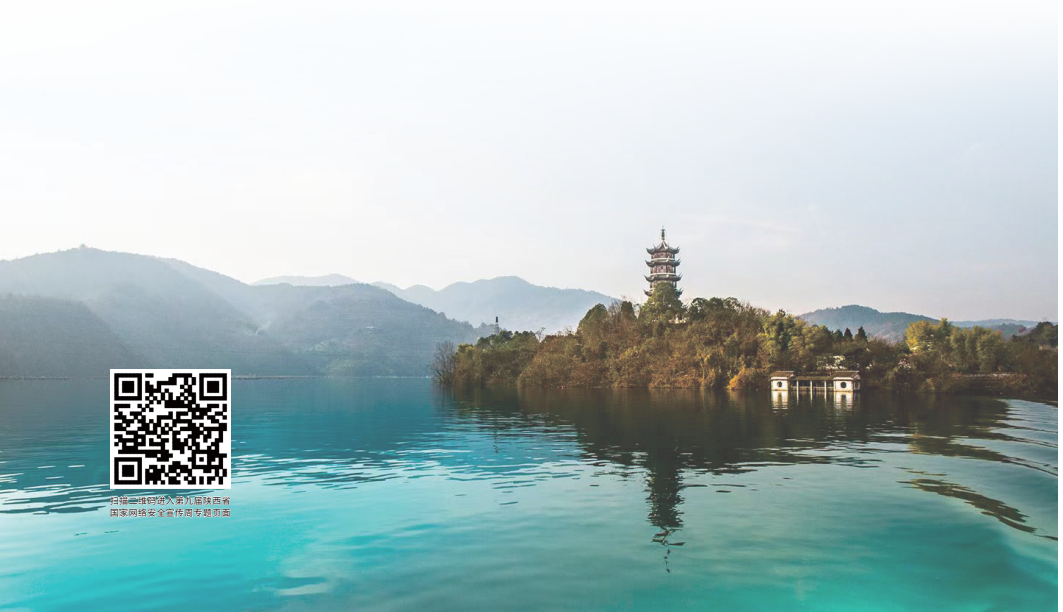
国家网络安全宣传周
China Cybersecurity Week

9TH

9月5日-9月11日

2022年陕西省第九届国家网络安全宣传周

THE NINTH NATIONAL CYBER SECURITY PUBLICITY WEEK OF SHAANXI PROVINCE



扫描二维码进入第九届陕西省国家网络安全宣传周专题页面

前 言

2022年国家网络安全宣传周将于2022年9月5日-11日举行，主题是“网络安全为人民，网络安全靠人民”，全国各省(直辖市、自治区)同步开展。陕西省第九届国家网络安全宣传周由省委宣传部、省委网信办、省教育厅、省公安厅、省通信管理局、省总工会、共青团陕西省委、省妇女联合会和中国人民银行西安分行等九部门联合举办。将深入宣传《网络安全法》、《数据安全法》、《个人信息保护法》、《关键信息基础设施安全保护条例》等法律法规，《网络安全审查办法》、《云计算服务安全评估办法》、《汽车数据安全管理若干规定（试行）》等法规政策文件，开展相关宣传活动，编写发放宣传资料，推动媒体、企业、社会团体广泛开展宣传普及，推进关键信息基础设施保护、大数据安全、个人信息保护等工作，通过展览、论坛、知识竞赛等多种形式，以及报刊、电台、电视台、网站等传播渠道，普及网络安全知识，提升全社会网络安全意识和防护技能，全面加强网络安全保障体系和能力建设，不断打造网络安全工作新格局。

“没有网络安全就没有国家安全，没有信息化就没有现代化”。网络安全和信息化已经成为事关国家安全、经济社会安全和国家发展的重大战略问题，要求我们必须贯彻以人民为中心的发展思想，本着对社会负责、对人民负责、对国家负责的态度，发展好网信事业、治理好网络空间、守护好这个亿万民众共同的精神家园，让互联网更好地造福人民。

中共陕西省委网信办
陕西省互联网信息办公室

陕西省第九届国家网络安全宣传周活动介绍

一、活动时间

2022年9月5日-11日

二、活动主题

网络安全为人民 网络安全靠人民

9.6 校园日　9.7 电信日　9.8 法制日

9.9 金融日　9.10 青少年日 9.11 个人信息保护日

三、举办单位

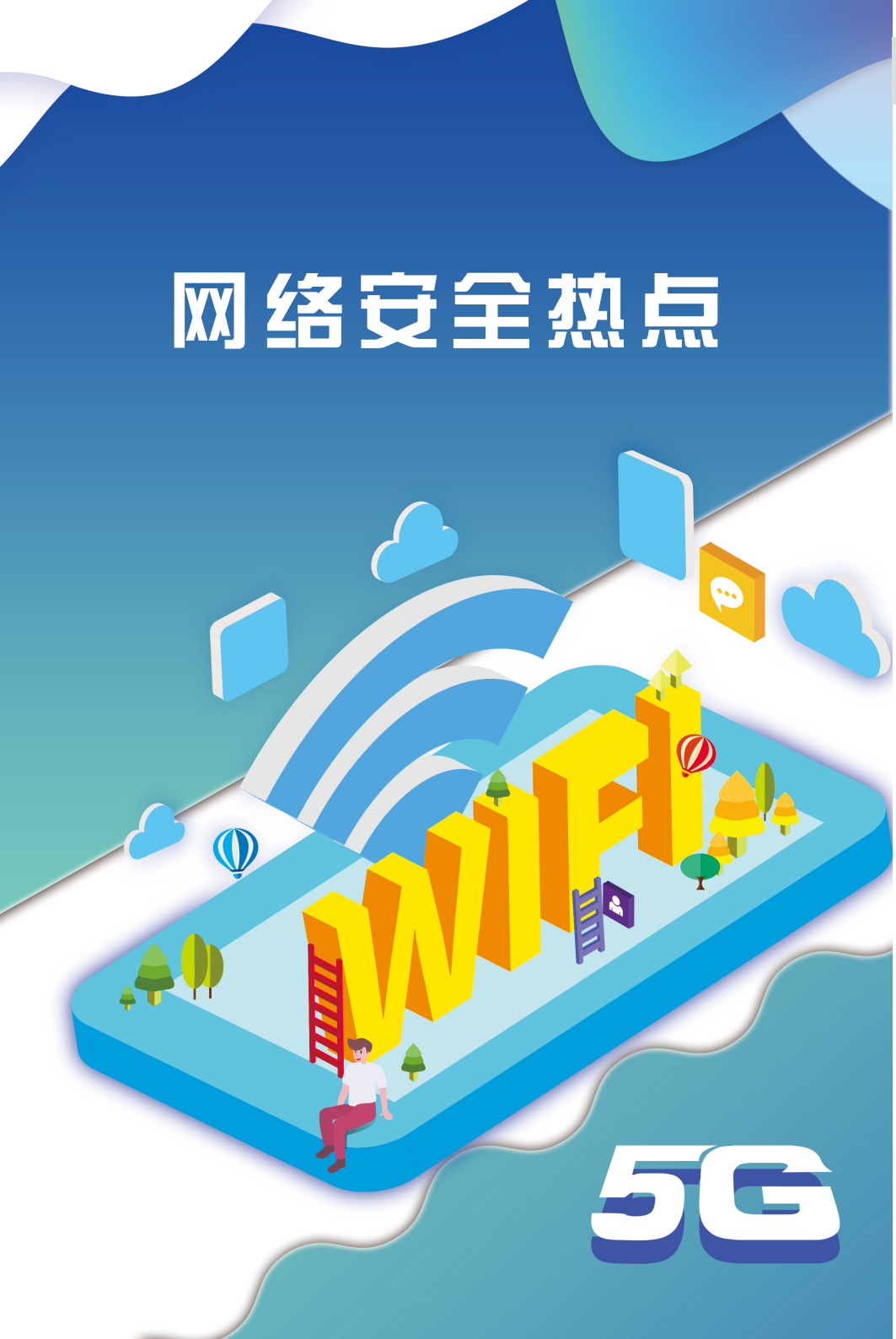
中共陕西省委宣传部、中共陕西省委网信办、陕西省教育厅、陕西省公安厅、陕西省通信管理局、陕西省总工会、共青团陕西省委、陕西省妇女联合会、中国人民银行西安分行

四、重要活动

开幕式、网络安全成果和技术应用展、网络安全大讲堂、主题日活动、网络安全进基层、网络安全安全技能竞赛

目录 CONTENTS

网络安全热点



1 网络安全法律法规体系逐步建立

“网络安全法是一部制定难度大、技术含量高的法律，也是一部实施良好的法律。”全国人大宪法和法律委员会副主任委员江必新认为，这部法律在制定过程中，涉及前沿科学技术、网络基础设施等一系列问题；近年来，有关部门依法处理了大量网络安全相关案件，也出台了一批配套规范性文件。

中国行政体制改革研究会副会长、中央党校（国家行政学院）教授汪玉凯表示，这部法律为互联网健康有序发展提供了保障，加快了网络空间治理体系和治理能力现代化进程。

在网络安全法实施之后，我国相继颁布《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《关键信息基础设施安全保护条例》等法律法规，出台《网络安全审查办法》《云计算服务安全评估办法》等政策文件，建立网络安全审查、云计算服务安全评估、数据安全管理、个人信息保护等一批重要制度，制定发布300余项网络安全领域国家标准，基本构建起网络安全政策法规体系的“四梁八柱”。

“一系列配套法规及相关实施标准的出台，形成了有中国特色的法律体系，对维护国家安全、网络主权，保护公民权利，促进数据流动应用及经济发展都起到了重要作用。”中国人民大学法学院教授张新宝说。

2 步入“新安全时代”，也面临更多新风险

5年来，我国网络安全产业发展迈入快车道，网络安全也不断融入产业数字化、数字产业化发展进程中。“随着数字化渗透到国家经济社会发展和个人生活的方方面面，我们需要把网络安全升级为数字安全，建立保障数字经济发展的数字安全屏障。”全国政协委员、360集团创始人周鸿祎说。

行业发展面临新风险、新挑战。“新的安全时代即将到来。”中国工程院院士邬贺铨认为，居家办公、远程学习推动网络环境开放、用户角色增加、防护边界扩张，带来各类新安全风险；5G商用推进工业互联网发展，企业内外网关联增加了工业互联网安全风险；智慧城市、物联网和车联网在开启万物互联的同时，城市安全越来越受重视……

针对具体风险场景，邬贺铨介绍，勒索病毒上升为主要威胁，形成了相对完整的商业产业链；数据安全问题严峻，尤其去年以来，跨境数据安全问题频发；开源代码安全面临隐患，很多共享代码没有经过安全设计和安全测试，常包含大量漏洞；云安全风险愈演愈烈，除一系列云原生安全攻击事件频发外，与云安全相关的挖矿劫持等也开始出现。

“网络空间已经成为大国博弈的战场，对关键基础设施提出新挑战、新课题，包括运行服务中断、通信基础设施瘫痪等问题。”中国移动信安中心总经理张滨强调，亟须重视我国关键信息基础设施保护，包括应对高等级网络攻击、大规模黑客组织威胁以及保障供应链安全等。

3 与时俱进、补齐短板，持续推进依法治网

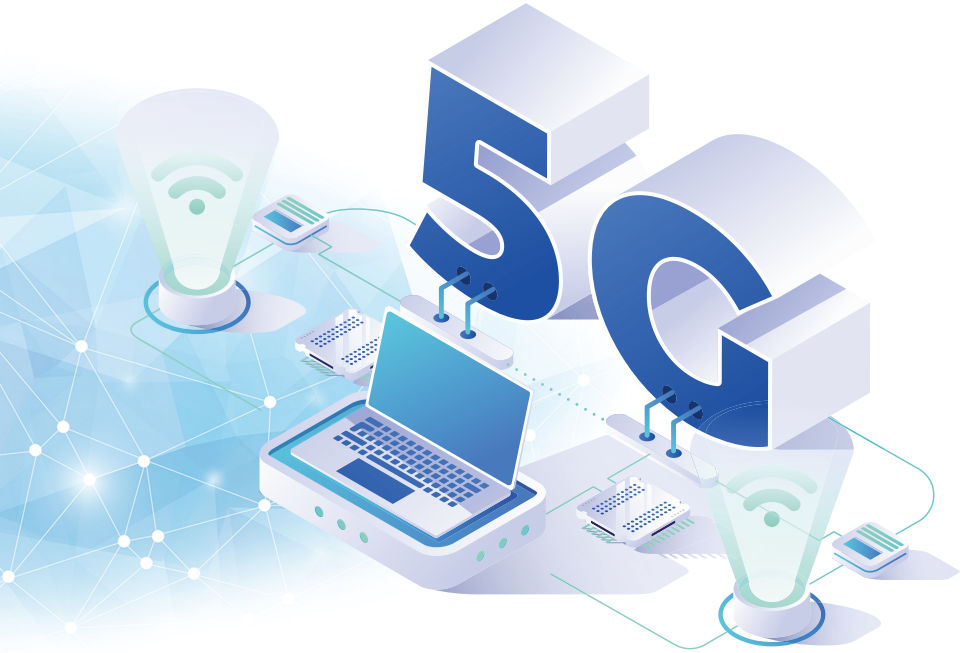
与新应用、新业态伴生的新问题需要法律规范，大量空白也需要法律填补。座谈会上，中国网络空间安全协会理事长王秀军表示，网络安全法治体系建设需要全行业、全社会共同推进。

在江必新看来，要从理念精神原则、法律调整对象、问题与制度对应、法律规范要素等方面进行体系化建构；通过树立善意实施和诚信实施的理念、建构实施规则、设置基本的互联网法律底线、综合运用立改废等手段，让网络安全法在实施中与时俱进、扬长避短。

此外，还要处理好法律之间的协调性。汪玉凯认为，在推进网络强国、数字中国建设进程中，要协调好网络安全法与配套规制的衔接，整合网络安全法的配套规制，防止政出多门，强化法理依据；还要加快弥补短板，解决“卡脖子”技术问题，为网络安全提供基础性保障。

在完善配套法规政策方面，张新宝建议，要对数据及个人信息出境，以及企业境外上市等领域加强执法监管；加强相关基础领域研究；加强网络信息安全和个人信息保护的法治教育。

中国工程院院士沈昌祥说：“要依照网络安全法，着眼国家安全和长远发展，构建世界领先、自立自强、安全可信的网络安全产业生态体系；积极构建网络空间安全防护体系，发展基于可信和支撑并行的，动态、实时、全方位的网络安全主动免疫能力；积极参与网络空间国际治理，加强网络空间国际合作，建立国家主权透明的国际互联网治理体系。”



网络技术安全

NETWORK SECURITY HANDBOOK

网络技术安全

有效规范算法应用 营造清朗网络空间

2022年4月8日起，中央网信办牵头开展“清朗·2022年算法综合治理”专项行动……过去一个时期，监管部门主动作为，全社会共同发力，算法乱象得到有效整治，算法应用日益朝着向上向善的轨道发展。

1 算法滥用，对公众产生不利影响

李明（化名）下载了一个以“知识分享”为主题的APP。打开后，一篇标记着“您可能感兴趣”的文章被推送至界面。

“这不恰好是我最关注的话题吗？”李明点进去一看，文章的观点“恰好”与自己的十分一致，让李明感觉“有理有据，令人信服”。李明看完一篇，系统又推荐了另一篇他感兴趣的文章。不知不觉，李明竟在该APP上一连“刷”了几个小时。

“这就是算法推荐的作用。”某公司软件工程师黄淑介绍，平台会抓取用户观看某话题总体评价的停留时间、留言时是正面还是负面倾向、“点赞”还是“反对”等信息来判定用户的内容偏好。此后，平台还会利用算法依据“内容相似度”和“用户相似度”，把你最可能感兴趣的内容推荐给你。

2 算法推荐的大规模使用，是否会对公众产生不利影响？

“算法推荐的个性化分发技术，较多地依赖总体热度、个体兴趣等数据。”复旦大学新闻学院副院长、教授周葆华介绍，目前对算法推荐的担忧主要在于：一方面平台追求更大传播热度，形成对内容价值观的忽视，如推荐低俗内容；另一方面基于对个性化兴趣和朋友关系的计算，信息推送与观点供给可能形成“回音室”效应，从而让用户深陷“信息茧房”中。

胡女士通过某APP向某酒店预订一个房间，支付价格近3000元。可入住后才发现，该房型的实际挂牌价仅1000多元。作为该平台“钻石贵宾客户”，胡女士非但没有享受到会员优惠，还支付了高于实际产品价格的费用。胡女士认为自己遭遇了“大数据杀熟”。她怀疑平台利用算法进行用户“画像”，根据自己对价格不敏感、不索要发票等消费习惯，抬高价格，欺诈销售，遂将该平台公司诉至法院。

据介绍，利用算法进行“大数据杀熟”的情形现实中不少见。例如购买同一班飞机票，自己花了上千元，别人同时购买却只花了几百元，这可能只是因为你已经是平台“熟客”，不再需要低价吸引等。

“有效治理算法乱象，是构建安全清朗的网络生态的必然要求。”中国政法大学副教授郑玉双表示，要健全算法的法律规制模式，破解算法的法律规制难题，实现算法善治。

3 建章立制，为算法立规矩树导向

“算法推荐的个性化分发技术，较多地依赖总体热度、个体兴趣等数据。”复旦大学新闻学院副院长、教授周葆华介绍，目前对算法推荐的担忧主要在于：一方面平台追求更大传播热度，形成对内容价值观的忽视，如推荐低俗内容；另一方面基于对个性化兴趣和朋友关系的计算，信息推送与观点供给可能形成“回音室”效应，从而让用户深陷“信息茧房”中。

胡女士通过某APP向某酒店预订一个房间，支付价格近3000元。可入住后才发现，该房型的实际挂牌价仅1000多元。作为该平台“钻石贵宾客户”，胡女士非但没有享受到会员优惠，还支付了高于实际产品价格的费用。胡女士认为自己遭遇了“大数据杀熟”。她怀疑平台利用算法进行用户“画像”，根据自己对价格不敏感、不索要发票等消费习惯，抬高价格，欺诈销售，遂将该平台公司诉至法院。

据介绍，利用算法进行“大数据杀熟”的情形现实中不少见。例如购买同一班飞机票，自己花了上千元，别人同时购买却只花了几百元，这可能只是因为你已经是平台“熟客”，不再需要低价吸引等。

此外，算法推荐还存在诸多其他问题。一些外卖等服务平台采用调度决策类算法进行工作调度时，过度追求工作效率和强度，按照最短可能用时设置配送员的配送时限，让“外卖小哥”为了按时送达而不得不超速、逆行等；有些平台还存在偏见歧视问题，将违法和不良信息关键词记入用户兴趣点；某些应用程序设置算法未经允许抓取用户个人信息……

“有效治理算法乱象，是构建安全清朗的网络生态的必然要求。”中国政法大学副教授郑玉双表示，要健全算法的法律规制模式，破解算法的法律规制难题，实现算法善治。

4 多元共治，引导算法向上向善

算法广泛而深入地应用于互联网，因此，算法治理绝不是凭一家之力就能实现的，必须全社会携手，建立多元共治的局面。

监管部门及时有效的政策举措，是规制算法乱象的有力武器。2022年3月1日起，互联网信息服务算法备案系统正式上线运行。根据相关要求，具有舆论属性或者社会动员能力的算法推荐服务提供者应当在提供服务之日起10个工作日内填报服务提供者的名称、服务形式、应用领域、算法类型、算法自评估报告等信息。

4月8日起，中央网信办牵头开展“清朗·2022年算法综合治理”专项行动，深入排查整改互联网企业平台算法安全问题，重点检查具有较强舆论属性或社会动员能力的大型网站、平台及产品等。

在算法治理过程中，司法发挥着引导行为、明确底线、稳定预期的重要作用。

“近年来，数起涉及算法推荐的司法案件引起社会关注，相关判决起到了为算法应用立规矩、树导向的作用。”西南政法大学副教授易健雄说。

此外，平台企业的行业自律也必不可少。

2021年10月22日，深圳市APP个人信息共护大会举行。20余家重点APP运营企业签署《深圳市APP个人信息保护自律承诺书》，承诺将保护用户公平交易权，不利用大数据“杀熟”；未经用户单独同意，不利用敏感个人信息进行线上精准营销和线下推销等。此前，国内10家互联网平台企业也签署承诺书，承诺不非法收集、使用消费者个人信息，不利用数据优势“杀熟”。建章立制，强化监管，鼓励自律……运用法治方法规范算法应用，引导算法向上向善，才能最大化促进社会公共利益，共同营造清朗安全的网络空间。

量子密钥分发网络可实现高安全性

日前，中国科学技术大学郭光灿院士团队在量子密钥分发网络化研究方面取得重要进展。该团队韩正甫教授及其合作者王双、银振强、陈巍等实现了抗环境干扰的非可信节点量子密钥分发网络，全面提高了量子密钥分发网络的安全性、可用性和可靠性，向实现下一代量子网络迈出了重要的一步。相关研究成果近日在线发表在国际知名学术期刊《光学》上。

网络安全是信息时代的重要主题，量子密钥分发网络以量子物理原理为基础，可为成千上万的用户提供信息论安全的保密通信服务，构建安全可控的网络环境。但网络中对于可信节点的需求提高了其实际部署的门槛，如何免除用户链路上必须可信的中间节点，降低对通信链路的安全性要求，从而构建下一代基于非可信节点的量子网络，是目前急需解决的问题。

在本研究中，课题组设计了“萨格纳克-马赫-曾德尔”结构的非相敏量子编码器，能够免除相位参考系的补偿。同时，课题组借助随机化，擦除了编码量子态的偏振信息，使其具备抗信道偏振扰动能力。最后，课题组重新利用偏振维度进行多用户配对，能够同步实现多对用户的Hong-Ou-Mandel干涉和联合测量。在此基础上，课题组完成了测量设备无关量子密钥分发网络的构建，使其同时具备抗环境干扰、无须可信节点、支持多用户灵活组网的特性。该成果推动了下一代量子保密通信网络的实用化，为未来量子互联网的具体形态做出了有益的探索。

为新技术应用加把安全锁（关注个人信息保护）

2020年，中共中央印发《法治社会建设实施纲要(2020—2025年)》。纲要提出，制定完善对“算法推荐、深度伪造等新技术应用的规范管理办法”。作为一项互联网新技术应用，深度伪造技术正越来越广泛地应用于现实场景，也出现被滥用错用的情况。推动技术的健康成长和使用，需构建更完善的法律和技术保护体系。

有一种技术，能对声音、影像进行篡改、伪造，从而实现“变声”“换脸”，并且高度逼真、很难甄别——这项互联网新技术叫做深度伪造技术。

借助人工智能技术可实现“换脸”“变声”

日常生活中，深度伪造技术的应用并不少见：智能客服的拟人回答、影视剧对角色的换脸处理……这些应用场景通过对图像、声音、视频的篡改、伪造和自动生成，产生高度逼真的效果。

深度伪造技术本质上是一种人工智能合成内容技术。据奇安信集团反金融犯罪专家卢维清介绍，起初，研究者使用自编码器实现对原始人脸的图像分解再还原。随着深度学习和先进算法的出现，深度伪造技术变得更加复杂成熟，除了图像，声音、视频都能被更精细地伪造或自动合成。以生成对抗网络算法为例，其同时搭载了生成器和鉴别器两个神经网络，前者基于一个数据库自动生成模拟该库中数据的样本，后者评估生成器生成数据的真伪，两者在互相博弈学习中产生大规模和高精确度的输出，实现真假难辨的效果。技术是一把双刃剑。深度伪造这项人工智能技术起初仅限于学术研究，后来广泛应用于多个现实场景，发挥着一定正面效应。

卢维清举例说，在教育场景中出现的虚拟教师和虚拟历史人物，能让数字教学更具互动性和代入感；影视制作通过还原或者修改角色镜头，降低修复成本，提高制作效率；虚拟新闻主播和客服，无需真人出现，可以降低人力投入；安防领域借此技术生成更加逼真的图像、视频，测试现有安全系统，寻找技术漏洞，助力更新迭代；娱乐休闲应用程序则可以对图片和视频做特效处理，增加趣味性……

但是，随着技术的发展及应用门槛的降低，许多个人用户也能轻松实现“换脸”“变声”，还有一些人将深度伪造技术应用于安全漏洞攻击、虚假音视频诈骗等，技术滥用带来的风险逐渐为人们所知。

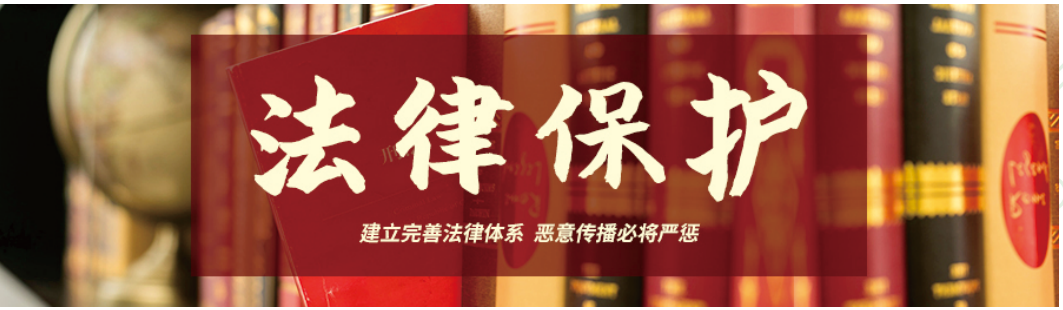
可能被诈骗、网络攻击等非法行为利用

此前，有国外网民利用换脸技术伪造艺人的影像资料并发布了视频，引发争议。

深度伪造技术被滥用的隐患，简单来说就是盗用他人的身份，让人“言”所未言、“行”所未行，以假乱真，混淆真相。

据专家介绍，若无有效的监管措施，任由深度伪造技术被滥用错用，社会生活中的每个人都存在被这项技术侵害的可能性。

例如，面部识别、声纹认证等生物特征识别机制有可能面临失效；公司企业可能被虚假消息欺诈，内部资料可能因为伪装登录而面临丢失、篡改、删除；有关部门在司法认证、证据收集、识别环节将面临真假难题；金融机构管理的账户可能遭遇伪装窃取，转移资金；电信诈骗里伪装公检法、银行、通信人员的手段会更加复杂，令人防不胜防……这些场景有可能带来一系列更深层次的社会问题。



构建更完善的法律和技术保护体系

2020年，中共中央印发《法治社会建设实施纲要(2020—2025年)》。纲要提出，制定完善对“算法推荐、深度伪造等新技术应用的规范管理办法”。今年3月，国家互联网信息办公室、公安部指导各地网信部门、公安机关加强对语音社交软件和涉“深度伪造”技术的互联网新技术新应用安全评估工作，并对未履行安全评估程序的11家企业进行约谈，引发社会关注。

面对深度伪造技术被滥用错用引发的犯罪和不良社会影响，专家建议，需尽快制定应对措施，防范化解风险。

宜鼓励研发鉴伪和溯源技术。卢维清认为，目前学术界和商业界的防伪开发项目多针对特定产品而非通用的音视频，还没有构建通用性的视频鉴伪网络。要加大对通用且高效鉴伪技术的研发投入和支持力度，鼓励科研院所和企业研究检测算法、主动防御算法、深度伪造图像和伪造语音的融合检测技术等。

宜加强对社会各界的科普。通过培训等方式让人们意识到深度伪造技术被滥用错用带来的危害，逐步提高用户的防范意识和鉴别能力，为相关鉴别技术的发展提供机会，促进深度伪造技术的合法利用。

宜加强相关司法体系的建立。专家建议，建立更加完整的法律法规体系，对恶意制作或传播的用户进行惩戒。2019年，国家互联网信息办公室发布《网络信息内容生态治理规定》，网络信息内容服务使用者和网络信息内容生产者、网络信息内容服务平台不得利用深度学习、虚拟现实等新技术新应用从事法律、行政法规禁止的活动。尽管已出台了相关法律法规遏制深度伪造技术的滥用，但还需要相关部门建立更加完整细致的法律体系，在区分伪造视频是属于娱乐还是恶性传播等问题上厘清边界，为新技术的应用划好红线。

对一般用户而言，由于不具有专业知识，很难识别出伪造的信息。尤其在技术发展迅速的背景下，专业人士也很难鉴别深度伪造的音视频。

卢维清建议，在有关财产、信用、安全等敏感问题的处理上，用户要更加谨慎，做好数据备份以便取证，对于不确定的情形及时联系官方客服或报警求助。

日常使用手机时，最好设置安全等级高的访问密码，拒绝打开陌生的网站和应用软件，尤其是系统提示有安全隐患的访问要及时停止，并定期对电脑系统杀毒，尽量减少在网上发布带有个人信息的图像、音视频等。如果身份证、驾驶证等有关个人安全和信息的物件丢失，要第一时间挂失。平时多学习法律知识，关键时刻采用法律武器维护个人的合法权益。

网络安全小百科

共建网络安全 共享网络文明

BUILD NETWORK SECURITY AND SHARE NETWORK CIVILIZATION

App能提取哪些个人信息？

近日，国家互联网信息办公室等四部门联合印发《常见类型移动互联网应用程序必要个人信息范围规定》，明确了39种常见类型App的必要个人信息范围，要求自2021年5月1日起，其运营者不得因用户不同意收集非必要个人信息，而拒绝用户使用App基本功能服务。“网信中国”今日为您梳理39种常见类型App的必要个人信息范围，一起来看。

地图导航类
位置信息
出发地
到达地

网约车类
注册用户电话
乘车人位置信息

网络支付类
注册用户电话
用户个人信息
银行卡号

网上购物类
购物信息
收货人信息
支付信息

餐饮外卖类
注册用户电话
收货人信息
支付信息

问诊挂号类
注册用户电话
患者信息
病情描述

网络安全审查办法

为了确保关键信息基础设施供应链安全，维护国家安全，国家互联网信息办公室、国家发展改革委等12部门联合制定了《网络安全审查办法》(以下简称《办法》)，将于2020年6月1日起实施。

1、审查的对象

关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，应当按照《办法》进行网络安全审查。

关键信息基础设施是什么?

电信、广播电视、能源、金融、公路水路运输、铁路、民航、邮政、水利、应急管理、卫生健康、社会保障、国防科技工业等重要行业和领域，一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的网络和信息系统。

网络产品和服务有哪些?

核心网络设备、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务，以及其他对关键信息基础设施安全有重要影响的网络产品和服务。

2、审查的重点

1、产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或破坏，以及重要数据被窃取、泄露、毁损的风险;

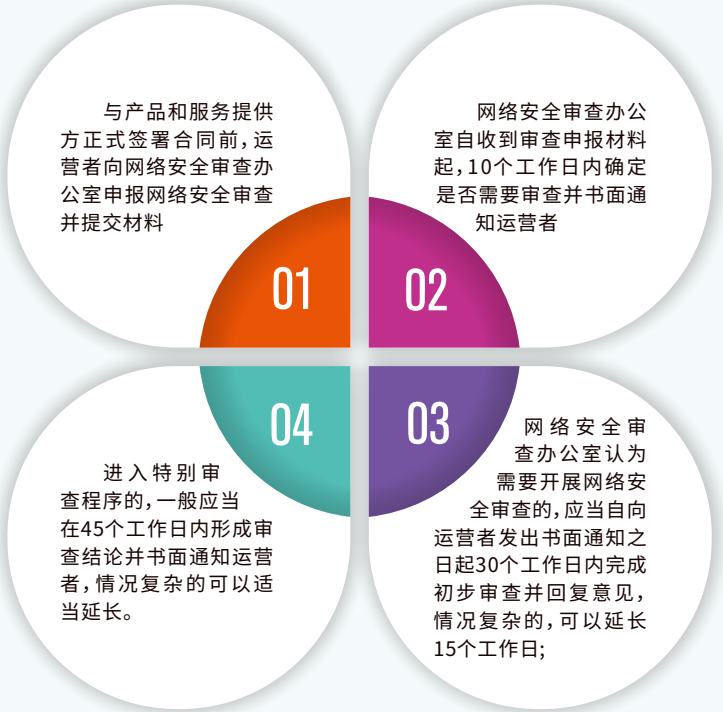
2、产品和服务供应中断对关键信息基础设施业务连续性的危害;

3、产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险;

4、产品和服务提供者遵守中国法律、行政法规、部门规章情况;

5、产品和服务提供者遵守中国法律、行政法规、部门规章情况;

3、审查的流程



4、违反“办法”规定应承担哪些法律责任?

根据《网络安全法》第六十五条规定，应当申报网络安全审查而没有申报的，或者使用网络安全审查未通过的产品和服务，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款;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。

最全的反诈骗知识来啦

诈骗手段层出不穷，反诈骗灵魂八问你已了解几个?

灵魂一问:刷单前问问自己,动动手指就能赚钱的好事,为啥能轮到你?

灵魂二问:网恋前问问自己,人靓声甜的小姐姐,温柔帅气又有钱的小哥哥,为啥还需要网恋?

灵魂三问:收到逮捕令时问问自己,抓人还需要提前通知,警察是不是觉得自己太闲,怕坏人跑路跑的不够快?

灵魂四问:裸聊前问问自己,自己的身材值不值得,美女与你“坦诚相见”?

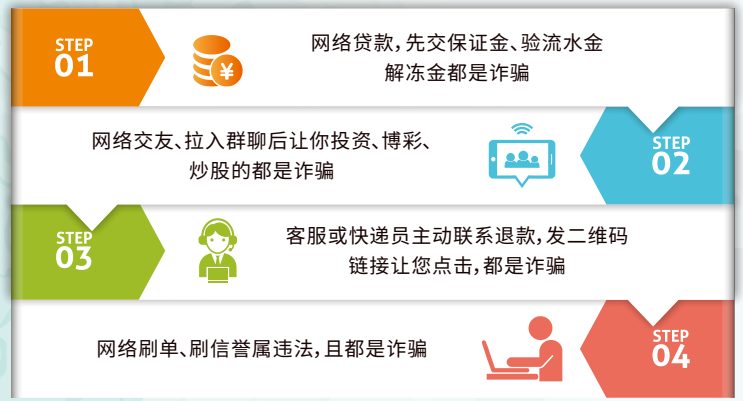
灵魂五问:网贷前问问自己,无抵押还免息,对方为啥不直接送钱给你?

灵魂六问:点陌生链接前问问自己,查信息就查信息,为啥还要下载一些东西?

灵魂七问:理财前问问自己,战无不胜的理财投资大师,为啥要苦口婆心帮助非亲非故的你?

灵魂八问:给领导转账前问问自己,用自己微信公然收受巨额资金,领导是嫌自己官儿干久了?

“四大诈骗”手段 多发高发,一定要小心提防!



再送给大家一个“六个一律 、八个凡是”防骗宝典

一律挂掉	网络刷单、刷信誉属违法,且都是诈骗
一律挂掉	谈到中奖
一律挂掉	谈到“电话转接公安局、法院
一律删掉	所有短信,但凡让点击链接的
一律不点	微信里不认识的人发来链接
一律是诈骗	一提到“安全账户”的

这些上网安全小常识你不可不知

人们的生活已经离不开互联网,因此带来的网络安全问题也不容忽视。如何防范木马病毒攻击?如何防范钓鱼网站?如何防范个人隐私泄露?看看这些上网安全常识。

1、日常安全陷阱

使用手机APP要谨慎

现象 现在恶意APP程序越来越多,各类非官方下载渠道常被恶意应用。

建议 不使用来历不明APP
安装时注意应用权限与产品是否相关

陌生人发微信红包勿乱点

现象 不法分子将手机病毒伪装成微信红包诱导消费者领取

建议 如果点击红包要填写个人信息等,肯定是骗局,及时修改密码删除病毒

人脸识别也危险

现象 两部手机、一张正面照和换脸APP,就能通过3D脸模骗过人脸识别系统

建议 在这项技术没有成熟之前,慎重使用

Wifi威胁真不少

现象 不法分子设置钓鱼WiFi热点,通过恶意程序监听劫持用户上网流量

建议 出门在外尽量使用4G网络,避免免费WiFi风险

2、防骗指南——五“不”、两“核实”

不轻信:所有利益诱导性信息都不要轻易理睬、所有装熟人的都不要轻易相信;

不回拨:陌生信息中提供的联系方式,都不要轻易致电联系;

不点击:只要是陌生网址,都不要点击;

不透露:手机号码、家庭住址、身份证号、银行卡账号密码、支付密码等一切个人隐私信息不可泄露;

不转账:房补、车补、中奖、退税、银行卡积分兑换现金等不要贪,身份不核实清楚不转账;

核实转账请求:他人要求借钱、打款、线上支付等,所有现金往来一定要当面或电话联系本人确认;

核实可以信息:陌生可疑的短信、电话、微信等,都通过线下营业厅、官方网站等官方渠道核实。

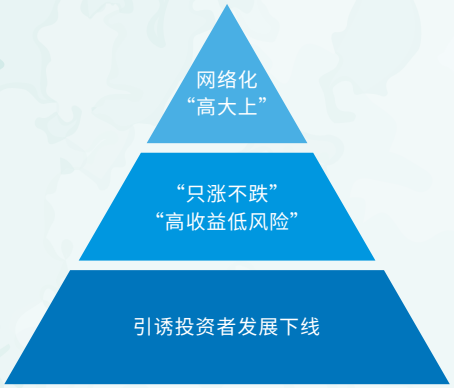
3、养成七个好习惯

- 保护好个人身份证和银行卡信息,保存好不用的复印件、交易流水信息
- 网上银行操作时,最好手工输入银行官方网站
- 开通账户动账通知短信,发现账户资金异动,立刻冻结或挂失
- 在取款输入密码时用手遮挡
- 密码要设置地相对复杂、独立,要定期更换
- 进行网上银行,支付账户操作时,不要随意连接不明公共WiFi
- 单独设立小额度银行账户,用于日常网上购物等消费

这些网络安全知识,你知道吗?

一些不法分子打着“金融创新”“区块链”的旗号,通过发行所谓“虚拟货币”“虚拟资产”“数字资产”等吸收资金,实则是炒作区块链概念,行非法集资、传销、诈骗之实。

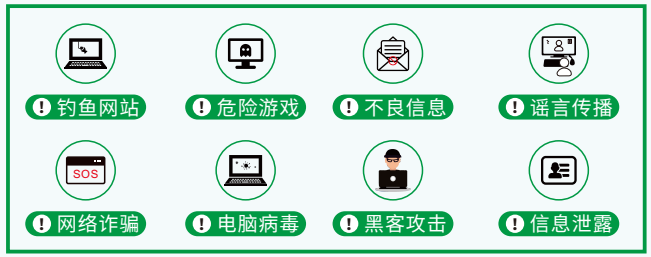
识别这种骗局,大家需要记住这**三大特点**:



青少年网络安全常识 你一定要知道

随着信息时代的到来,互联网已渗透到我们生活的方方面面。在这个拥有浩瀚资源的虚拟空间里,我们可以学到许多书本上没有的知识,但与之伴生的网络安全威胁也不容忽视。提升自身的网络安全意识,增强网络安全防御能力刻不容缓。

网络安全隐患



安全上网指南

- 电脑定期杀毒,定期修改并使用安全强度高的密码。
- 妥善保管个人隐私信息、账号及密码,谨慎发布个人信息。
- 到知名正规的网站购物,不轻易向对方付款或提供银行卡密码。
- 文明、绿色、健康上网,浏览正规的网站和栏目。
- 远离网络上的暴力渲染、色情诱惑、钱财赌博、灰色游戏等内容。

预防孩子沉迷游戏

家长以身作则
不做低头族

控制孩子上网时间,
不将游戏当精神寄托

多陪伴孩子,
给予更多关注

培养孩子兴趣
爱好

温馨提示

互联网已经渗透我们生活的方方面面,网络安全和每个人都息息相关。每个人都要提高网络安全意识,共建互联网清朗空间。

如何做好个人信息保护?

互联网时代,个人信息的重要性不言而喻,而无孔不入的信息泄露风险使我们不得不提高警惕。下面,网警以什么是个人信息、如何防范个人信息泄露,带你走进个人信息保护日。

1、什么是个人信息?

1.个人身份信息:包括个人姓名、性别、国籍、民族身份证件种类号码及有效期限、职业联系方式婚姻获说、家庭状说、往所或工作单位地址及照片等;

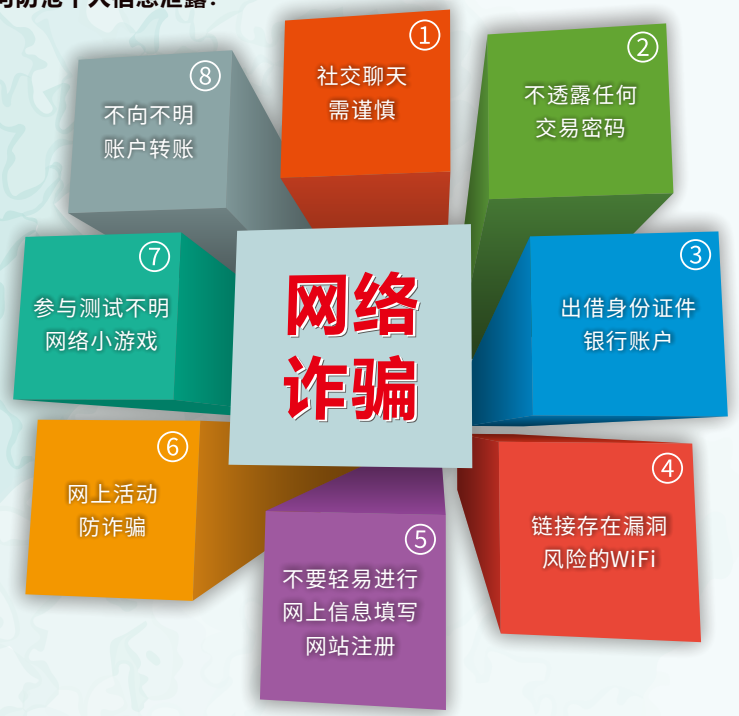
2个人账户信息:包括账号、账户开立时间、开户行、账户余额、账户交易、以及在金融机构支付结算理财、保险箱等中间业务过程中获取、保存、留存的个人信息等;

3.个人信用信息:包括信用卡还款情况、贷款偿还情况以及个人在经济活动中形成的,能够反映其信用状况的其他信息;

4.个人隐私信息:通讯录信息、通话记录、短信记录、聊天记泉、购物信息记录、个大视频、照片等;

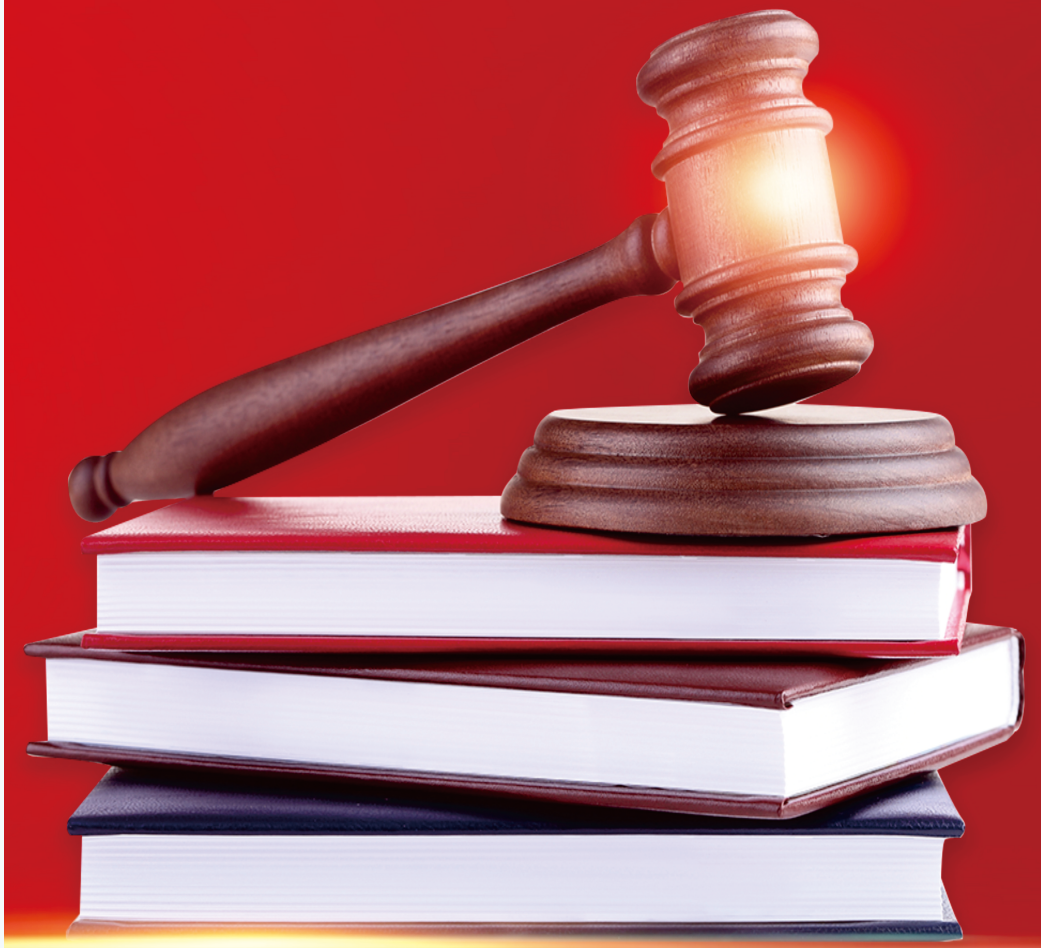
5衍生信息:包括个人消费习惯、投资意愿等对原始信息进行处理、分析所形成的反映特定个人某些情况的信息 以及你的设备信息、社会关系信息、网络行为信息等。

2、如何防范个人信息泄露?



法律法规知识

— KNOWLEDGE OF LAWS AND REGULATIONS —



中华人民共和国数据安全法

第一章 总 则

第一条 为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，制定本法。

第二条 在中华人民共和国境内开展数据处理活动及其安全监管，适用本法。

在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。

第三条 本法所称数据，是指任何以电子或者其他方式对信息的记录。

数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。

数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

第四条 维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。

第五条 中央国家安全领导机构负责国家数据安全工作的决策和议事协调，研究制定、指导实施国家数据安全战略和有关重大方针政策，统筹协调国家数据安全的重大事项和重要工作，建立国家数据安全工作协调机制。

第六条 各地区、各部门对本地区、本部门工作中收集和产生的数据及数据安全负责。

工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。

公安机关、国家安全机关等依照本法和有关法律、行政法规的规定，在各自职责范围内承担数据安全监管职责。

国家网信部门依照本法和有关法律、行政法规的规定，负责统筹协调网络数据安全和相关监管工作。

第七条 国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展。

第八条 开展数据处理活动，应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。

第九条 国家支持开展数据安全知识宣传普及，提高全社会的数据安全保护意识和水平，推动有关部门、行业组织、科研机构、企业、个人等共同参与数据安全保护工作，形成全社会共同维护数据安全和促进发展的良好环境。

第十条 相关行业组织按照章程，依法制定数据安全行为规范和团体标准，加强行业自律，指导会员加强数据安全保护，提高数据安全保护水平，促进行业健康发展。

第十一条 国家积极开展数据安全治理、数据开发利用等领域的国际交流与合作，参与数据安全相关国际规则和标准的制定，促进数据跨境安全、自由流动。

第十二条 任何个人、组织都有权对违反本法规定的行为向有关主管部门投诉、举报。收到投诉、举报的部门应当及时依法处理。

有关主管部门应当对投诉、举报人的相关信息予以保密，保护投诉、举报人的合法权益。

第二章 数据安全与发展

第十三条 国家统筹发展和安全，坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展。

第十四条 国家实施大数据战略，推进数据基础设施建设，鼓励和支持数据在各行业、各领域的创新应用。

省级以上人民政府应当将数字经济发展纳入本级国民经济和社会发展规划，并根据需要制定数字经济发展规划。

第十五条 国家支持开发利用数据提升公共服务的智能化水平。提供智能化公共服务，应当充分考虑老年人、残疾人的需求，避免对老年人、残疾人的日常生活造成障碍。

第十六条 国家支持数据开发利用和数据安全技术研究，鼓励数据开发利用和数据安全等领域的技术推广和商业创新，培育、发展数据开发利用和数据安全产品、产业体系。

第十七条 国家推进数据开发利用技术和数据安全标准体系建设。国务院标准化行政主管部门和国务院有关部门根据各自的职责，组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准。国家支持企业、社会团体和教育、科研机构等参与标准制定。

第十八条 国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动。

国家支持有关部门、行业组织、企业、教育和科研机构、有关专业机构等在数据安全风险评估、防范、处置等方面开展协作。

第十九条 国家建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场。

第二十条 国家支持教育、科研机构和企业等开展数据开发利用技术和数据安全相关教育和培训，采取多种方式培养数据开发利用技术和数据安全专业人才，促进人才交流。

第三章 数据安全制度

第二十一条 国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。

关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。

各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

第二十二条 国家建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制。国家数据安全工作协调机制统筹协调有关部门加强数据安全风险信息的获取、分析、研判、预警工作。

第二十三条 国家建立数据安全应急处置机制。发生数据安全事件，有关主管部门应当依法启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。

第二十四条 国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查。

依法作出的安全审查决定为最终决定。

第二十五条 国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制。

第二十六条 任何国家或者地区在与数据和数据开发利用技术等有关的投资、贸易等方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。

第四章 数据安全保护义务

第二十七条 开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。

第二十八条 开展数据处理活动以及研究开发数据新技术，应当有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理。

第二十九条 开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

第三十条 重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。

风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

第三十一条 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；其他数据处理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办法，由国家网信部门会同国务院有关部门制定。

第三十二条 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。

第三十三条 从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。

第三十四条 法律、行政法规规定提供数据处理相关服务应当取得行政许可的，服务提供者应当依法取得许可。

第三十五条 公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的批准手续，依法进行，有关组织、个人应当予以配合。

第三十六条 中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据的请求。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。

第五章 政务数据安全与开放

第三十七条 国家大力推进电子政务建设，提高政务数据的科学性、准确性、时效性，提升运用数据服务经济社会发展的能力。

第三十八条 国家机关为履行法定职责的需要收集、使用数据，应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序进行；对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供。

第三十九条 国家机关应当依照法律、行政法规的规定，建立健全数据安全管理制度，落实数据安全保护责任，保障政务数据安全。

第四十条 国家机关委托他人建设、维护电子政务系统，存储、加工政务数据，应当经过严格的批准程序，并应当监督受托方履行相应的数据安全保护义务。受托方应当依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供政务数据。

第四十一条 国家机关应当遵循公正、公平、便民的原则，按照规定及时、准确地公开政务数据。依法不予公开的除外。

第四十二条 国家制定政务数据开放目录，构建统一规范、互联互通、安全可控的政务数据开放平台，推动政务数据开放利用。

第四十三条 法律、法规授权的具有管理公共事务职能的组织为履行法定职责开展数据处理活动，适用本章规定。

第六章 法律责任

第四十四条 有关主管部门在履行数据安全监管职责中，发现数据处理活动存在较大安全风险的，可以按照规定的权限和程序对有关组织、个人进行约谈，并要求有关组织、个人采取措施进行整改，消除隐患。

第四十五条 开展数据处理活动的组织、个人不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的，由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

违反国家核心数据管理制度，危害国家主权、安全和发展利益的，由有关主管部门处二百万元以上一千万元以下罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。

第四十六条 违反本法第三十一条规定，向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，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。

第四十七条 从事数据交易中介服务的机构未履行本法第三十三条规定的义务的，由有关主管部门责令改正，没收违法所得，处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足十万元的，处十万元以上一百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第四十八条 违反本法第三十五条规定，拒不配合数据调取的，由有关主管部门责令改正，给予警告，并处五万元以上五十万元以下罚款，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。

违反本法**第三十六条**规定，未经主管机关批准向外国司法或者执法机构提供数据的，由有关主管部门给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；造成严重后果的，处一百万元以上五百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上五十万元以下罚款。

第四十九条 国家机关不履行本法规定的数据安全保护义务的，对直接负责的主管人员和其他直接责任人员依法给予处分。

第五十条 履行数据安全监管职责的国家工作人员玩忽职守、滥用职权、徇私舞弊的，依法给予处分。

第五十一条 窃取或者以其他非法方式获取数据，开展数据处理活动排除、限制竞争，或者损害个人、组织合法权益的，依照有关法律、行政法规的规定处罚。

第五十二条 违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七章 附 则

第五十三条 开展涉及国家秘密的数据处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。

在统计、档案工作中开展数据处理活动，开展涉及个人信息的数据处理活动，还应当遵守有关法律、行政法规的规定。

第五十四条 军事数据安全保护的办法，由中央军事委员会依据本法另行制定。

第五十五条 本法自2021年9月1日起施行。

中华人民共和国个人信息保护法

第一章 总 则

第一条 为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，根据宪法，制定本法。

第二条 自然人的个人信息受法律保护，任何组织、个人不得侵害自然人的个人信息权益。

第三条 在中华人民共和国境内处理自然人个人信息的活动，适用本法。

在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法：

（一）以向境内自然人提供产品或者服务为目的；

（二）分析、评估境内自然人的行为；

（三）法律、行政法规规定的其他情形。

第四条 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，不包括匿名化处理后的信息。

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、删除等。

第五条 处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。

第六条 处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。

收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。

第七条 处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围。

第八条 处理个人信息应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。

第九条 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。

第十条 任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

第十一条 国家建立健全个人信息保护制度，预防和惩治侵害个人信息权益的行为，加强个人信息保护宣传教育，推动形成政府、企业、相关社会组织、公众共同参与个人信息保护的良好环境。

第十二条 国家积极参与个人信息保护国际规则的制定，促进个人信息保护方面的国际交流与合作，推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等互认。

第二章 个人信息处理规则

第一节 一般规定

第十三条 符合下列情形之一的，个人信息处理者方可处理个人信息：

（一）取得个人的同意；

（二）为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需；

（三）为履行法定职责或者法定义务所必需；

（四）为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；

（五）为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；

（六）依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；

（七）法律、行政法规规定的其他情形。

依照本法其他有关规定，处理个人信息应当取得个人同意，但是有前款第二项至第七项规定情形的，不需取得个人同意。

第十四条 基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。

个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意。

第十五条 基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。

个人撤回同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

第十六条 个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外。

第十七条 个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项：

（一）个人信息处理者的名称或者姓名和联系方式；

（二）个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；

（三）个人行使本法规定权利的方式和程序；

（四）法律、行政法规规定应当告知的其他事项。

前款规定事项发生变更的，应当将变更部分告知个人。

个人信息处理者通过制定个人信息处理规则的方式告知第一款规定事项的，处理规则应当公开，并且便于查阅和保存。

第十八条 个人信息处理者处理个人信息，有法律、行政法规规定应当保密或者不需要告知的情形的，可以不向个人告知前条第一款规定的事项。

紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的，个人信息处理者应当在紧急情况消除后及时告知。

第十九条 除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间。

第二十条 两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的，应当约定各自的权利和义务。但是，该约定不影响个人向其中任何一个个人信息处理者要求行使本法规定的权利。

个人信息处理者共同处理个人信息，侵害个人信息权益造成损害的，应当依法承担连带责任。

第二十一条 个人信息处理者委托处理个人信息的，应当与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督。

受托人应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息；委托合同不生效、无效、被撤销或者终止的，受托人应当将个人信息返还个人信息处理者或者予以删除，不得保留。

未经个人信息处理者同意，受托人不得转委托他人处理个人信息。

第二十二条 个人信息处理者因合并、分立、解散、被宣告破产等原因需要转移个人信息的，应当向个人告知接收方的名称或者姓名和联系方式。接收方应当继续履行个人信息处理者的义务。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。

第二十三条 个人信息处理者向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。

第二十四条 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。

通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。

通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。

第二十五条 个人信息处理者不得公开其处理的个人信息，取得个人单独同意的除外。

第二十六条 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、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。

第二十七条 个人信息处理者可以在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；个人明确拒绝的除外。个人信息处理者处理已公开的个人信息，对个人权益有重大影响的，应当依照本法规定取得个人同意。

第二节 敏感个人信息的处理规则

第二十八条 敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

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，个人信息处理者方可处理敏感个人信息。

第二十九条 处理敏感个人信息应当取得个人的单独同意；法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。

第三十条 个人信息处理者处理敏感个人信息的，除本法第十七条第一款规定的事项外，还应当向个人告知处理敏感个人信息的必要性以及对个人权益的影响；依照本法规定可以不向个人告知的除外。

第三十一条 个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。

个人信息处理者处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则。

第三十二条 法律、行政法规对处理敏感个人信息规定应当取得相关行政许可或者作出其他限制的，从其规定。

第三节 国家机关处理个人信息的特别规定

第三十三条 国家机关处理个人信息的活动，适用本法；本节有特别规定的，适用本节规定。

第三十四条 国家机关为履行法定职责处理个人信息，应当依照法律、行政法规规定的权限、程序进行，不得超出履行法定职责所必需的范围和限度。

第三十五条 国家机关为履行法定职责处理个人信息，应当依照本法规定履行告知义务；有本法第十八条第一款规定的情形，或者告知将妨碍国家机关履行法定职责的除外。

第三十六条 国家机关处理的个人信息应当在中华人民共和国境内存储；确需向境外提供的，应当进行安全评估。安全评估可以要求有关部门提供支持与协助。

第三十七条 法律、法规授权的具有管理公共事务职能的组织为履行法定职责处理个人信息，适用本法关于国家机关处理个人信息的规定。

第三章 个人信息跨境提供的规则

第三十八条 个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：

（一）依照本法第四十条的规定通过国家网信部门组织的安全评估；

（二）按照国家网信部门的规定经专业机构进行个人信息保护认证；

（三）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；

（四）法律、行政法规或者国家网信部门规定的其他条件。

中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。

个人信息处理者应当采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准。

第三十九条 个人信息处理者向中华人民共和国境外提供个人信息的，应当向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项，并取得个人的单独同意。

第四十条 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个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。

第四十一条 中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供存储于境内个人信息的请求。非经中华人民共和国主管机关批准，个人信息处理者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个人信息。

第四十二条 境外的组织、个人从事侵害中华人民共和国公民的个人信息权益，或者危害中华人民共和国国家安全、公共利益的个人信息处理活动的，国家网信部门可以将其列入限制或者禁止个人信息提供清单，予以公告，并采取限制或者禁止向其提供个人信息等措施。

第四十三条 任何国家或者地区在个人信息保护方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。

第四章 个人在个人信息处理活动中的权利

第四十四条 个人对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理；法律、行政法规另有规定的除外。

第四十五条 个人有权向个人信息处理者查阅、复制其个人信息；有本法第十八条第一款、第三十五条规定情形的除外。

个人请求查阅、复制其个人信息的，个人信息处理者应当及时提供。

个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。

第四十六条 个人发现其个人信息不准确或者不完整的，有权请求个人信息处理者更正、补充。

个人请求更正、补充其个人信息的，个人信息处理者应当对其个人信息予以核实，并及时更正、补充。

第四十七条 有下列情形之一的，个人信息处理者应当主动删除个人信息；个人信息处理者未删除的，个人有权请求删除：

（一）处理目的已实现、无法实现或者为实现处理目的不再必要；

（二）个人信息处理者停止提供产品或者服务，或者保存期限已届满；

（三）个人撤回同意；

（四）个人信息处理者违反法律、行政法规或者违反约定处理个人信息；

（五）法律、行政法规规定的其他情形。

法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理。

第四十八条 个人有权要求个人信息处理者对其个人信息处理规则进行解释说明。

第四十九条 自然人死亡的，其近亲属为了自身的合法、正当利益，可以对死者的相关个人信息行使本章规定的查阅、复制、更正、删除等权利；死者生前另有安排的除外。

第五十条 个人信息处理者应当建立便捷的个人行使权利的申请受理和处理机制。拒绝个人行使权利的请求的，应当说明理由。

个人信息处理者拒绝个人行使权利的请求的，个人可以依法向人民法院提起诉讼。

第五章 个人信息处理者的义务

第五十一条 个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失：

（一）制定内部管理制度和操作规程；

（二）对个人信息实行分类管理；

（三）采取相应的加密、去标识化等安全技术措施；

（四）合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；

（五）制定并组织实施个人信息安全事件应急预案；

（六）法律、行政法规规定的其他措施。

第五十二条 处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。

个人信息处理者应当公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。

第五十三条 本法第三条第二款规定的中华人民共和国境外的个人信息处理者，应当在中华人民共和国境内设立专门机构或者指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。

第五十四条 个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。

第五十五条 有下列情形之一的，个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录：

（一）处理敏感个人信息；

（二）利用个人信息进行自动化决策；

（三）委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；

（四）向境外提供个人信息；

（五）其他对个人权益有重大影响的个人信息处理活动。

第五十六条 个人信息保护影响评估应当包括下列内容：

（一）个人信息的处理目的、处理方式等是否合法、正当、必要；

（二）对个人权益的影响及安全风险；

（三）所采取的保护措施是否合法、有效并与风险程度相适应。

个人信息保护影响评估报告和处理情况记录应当至少保存三年。

第五十七条 发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项：

（一）发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害；

（二）个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施；

（三）个人信息处理者的联系方式。

个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的，个人信息处理者可以不通知个人；履行个人信息保护职责的部门认为可能造成危害的，有权要求个人信息处理者通知个人。

第五十八条 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，应当履行下列义务：

（一）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；

（二）遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务；

（三）对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务；

（四）定期发布个人信息保护社会责任报告，接受社会监督。

第五十九条 接受委托处理个人信息的受托人，应当依照本法和有关法律、行政法规的规定，采取必要措施保障所处理的个人信息的安全，并协助个人信息处理者履行本法规定的义务。

第六章 履行个人信息保护职责的部门

第六十条 国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。国务院有关部门依照本法和有关法律、行政法规的规定，在各自职责范围内负责个人信息保护和监督管理工作。

县级以上地方人民政府有关部门的个人信息保护和监督管理职责，按照国家有关规定确定。

前两款规定的部门统称为履行个人信息保护职责的部门。

第六十一条 履行个人信息保护职责的部门履行下列个人信息保护职责：

（一）开展个人信息保护宣传教育，指导、监督个人信息处理者开展个人信息保护工作；

（二）接受、处理与个人信息保护有关的投诉、举报；

（三）组织对应用程序等个人信息保护情况进行测评，并公布测评结果；

（四）调查、处理违法个人信息处理活动；

（五）法律、行政法规规定的其他职责。

第六十二条 国家网信部门统筹协调有关部门依据本法推进下列个人信息保护工作：

（一）制定个人信息保护具体规则、标准；

（二）针对小型个人信息处理者、处理敏感个人信息以及人脸识别、人工智能等新技术、新应用，制定专门的个人信息保护规则、标准；

（三）支持研究开发和推广应用安全、方便的电子身份认证技术，推进网络身份认证公共服务建设；

（四）推进个人信息保护社会化服务体系建设，支持有关机构开展个人信息保护评估、认证服务；

（五）完善个人信息保护投诉、举报工作机制。

第六十三条 履行个人信息保护职责的部门履行个人信息保护职责，可以采取下列措施：

（一）询问有关当事人，调查与个人信息处理活动有关的情况；

（二）查阅、复制当事人与个人信息处理活动有关的合同、记录、账簿以及其他有关资料；

（三）实施现场检查，对涉嫌违法的个人信息处理活动进行调查；

（四）检查与个人信息处理活动有关的设备、物品；对有证据证明是用于违法个人信息处理活动的设备、物品，向本部门主要负责人书面报告并经批准，可以查封或者扣押。

履行个人信息保护职责的部门依法履行职责，当事人应当予以协助、配合，不得拒绝、阻挠。

第六十四条 履行个人信息保护职责的部门在履行职责中，发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，可以按照规定的权限和程序对该个人信息处理者的法定代表人或者主要负责人进行约谈，或者要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。个人信息处理者应当按照要求采取措施，进行整改，消除隐患。

履行个人信息保护职责的部门在履行职责中，发现违法处理个人信息涉嫌犯罪的，应当及时移送公安机关依法处理。

第六十五条 任何组织、个人有权对违法个人信息处理活动向履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理，并将处理结果告知投诉、举报人。

履行个人信息保护职责的部门应当公布接受投诉、举报的联系方式。

第七章 法律责任

第六十六条 违反本法规定处理个人信息，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。

有前款规定的违法行为，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。

第六十七条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第六十八条 国家机关不履行本法规定的个人信息保护义务的，由其上级机关或者履行个人信息保护职责的部门责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

履行个人信息保护职责的部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第六十九条 处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。

前款规定的损害赔偿责任按照个人因此受到的损失或者个人信息处理者因此获得的利益确定；个人因此受到的损失和个人信息处理者因此获得的利益难以确定的，根据实际情况确定赔偿数额。

第七十条 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。

第七十一条 违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七章 法律责任

第七十二条 自然人因个人或者家庭事务处理个人信息的，不适用本法。

法律对各级人民政府及其有关部门组织实施的统计、档案管理活动中的个人信息处理有规定的，适用其规定。

第七十三条 本法下列用语的含义：

（一）个人信息处理者，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。

（二）自动化决策，是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。

（三）去标识化，是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。

（四）匿名化，是指个人信息经过处理无法识别特定自然人且不能复原的过程。

第七十四条 本法自2021年11月1日起施行。

关键信息基础设施安全保护条例

第一章 总 则

第一条 为了保障关键信息基础设施安全，维护网络安全，根据《中华人民共和国网络安全法》，制定本条例。

第二条 本条例所称关键信息基础设施，是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

第三条 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。

第四条 关键信息基础设施安全保护坚持综合协调、分工负责、依法保护，强化和落实关键信息基础设施运营者（以下简称运营者）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。

第五条 国家对关键信息基础设施实行重点保护，采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治危害关键信息基础设施安全的违法犯罪活动。

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。

第六条 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。

第七条 对在关键信息基础设施安全保护工作中取得显著成绩或者作出突出贡献的单位和个人，按照国家有关规定给予表彰。

第二章 关键信息基础设施认定

第八条 本条例第二条涉及的重要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（以下简称保护工作部门）。

第九条 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，并报国务院公安部门备案。

制定认定规则应当主要考虑下列因素：

（一）网络设施、信息系统等对于本行业、本领域关键核心业务的重要程度；

（二）网络设施、信息系统等一旦遭到破坏、丧失功能或者数据泄露可能带来的危害程度；

（三）对其他行业和领域的关联性影响。

第十条 保护工作部门根据认定规则负责组织认定本行业、本领域的关键信息基础设施，及时将认定结果通知运营者，并通报国务院公安部门。

第十一条 关键信息基础设施发生较大变化，可能影响其认定结果的，运营者应当及时将相关情况报告保护工作部门。保护工作部门自收到报告之日起3个月内完成重新认定，将认定结果通知运营者，并通报国务院公安部门。

第三章 运营者责任义务

第十二条 安全保护措施应当与关键信息基础设施同步规划、同步建设、同步使用。

第十三条 运营者应当建立健全网络安全保护制度和责任制，保障人力、财力、物力投入。运营者的主要负责人对关键信息基础设施安全保护负总责，领导关键信息基础设施安全保护和重大网络安全事件处置工作，组织研究解决重大网络安全问题。

第十四条 运营者应当设置专门安全管理机构，并对专门安全管理机构负责人和关键岗位人员进行安全背景审查。审查时，公安机关、国家安全机关应当予以协助。

第十五条 专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，履行下列职责：

（一）建立健全网络安全管理、评价考核制度，拟订关键信息基础设施安全保护计划；

（二）组织推动网络安全防护能力建设，开展网络安全监测、检测和风险评估；

（三）按照国家及行业网络安全事件应急预案，制定本单位应急预案，定期开展应急演练，处置网络安全事件；

（四）认定网络安全关键岗位，组织开展网络安全工作考核，提出奖励和惩处建议；

（五）组织网络安全教育、培训；

（六）履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度；

（七）对关键信息基础设施设计、建设、运行、维护等服务实施安全管理；

（八）按照规定报告网络安全事件和重要事项。

第十六条 运营者应当保障专门安全管理机构的运行经费、配备相应的人员，开展与网络安全和信息化有关的决策应当有专门安全管理机构人员参与。

第十七条 运营者应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，并按照保护工作部门要求报送情况。

第十八条 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，运营者应当按照有关规定向保护工作部门、公安机关报告。

第十九条 运营者应当优先采购安全可信的网络产品和服务；采购网络产品和服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查。

第二十条 运营者采购网络产品和服务，应当按照国家有关规定与网络产品和服务提供者签订安全保密协议，明确提供者的技术支持和安全保密义务与责任，并对义务与责任履行情况进行监督。

第二十一条 运营者发生合并、分立、解散等情况，应当及时报告保护工作部门，并按照保护工作部门的要求对关键信息基础设施进行处置，确保安全。

第四章 保障和促进

第二十二条 保护工作部门应当制定本行业、本领域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。

第二十三条 国家网信部门统筹协调有关部门建立网络安全信息共享机制，及时汇总、研判、共享、发布网络安全威胁、漏洞、事件等信息，促进有关部门、保护工作部门、运营者以及网络安全服务机构等之间的网络安全信息共享。

第二十四条 保护工作部门应当建立健全本行业、本领域的关键信息基础设施网络安全监测预警制度，及时掌握本行业、本领域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。

第二十五条 保护工作部门应当按照国家网络安全事件应急预案的要求，建立健全本行业、本领域的网络安全事件应急预案，定期组织应急演练；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。

第二十六条 保护工作部门应当定期组织开展本行业、本领域关键信息基础设施网络安全检查检测，指导监督运营者及时整改安全隐患、完善安全措施。

第二十七条 国家网信部门统筹协调国务院公安部门、保护工作部门对关键信息基础设施进行网络安全检查检测，提出改进措施。

有关部门在开展关键信息基础设施网络安全检查时，应当加强协同配合、信息沟通，避免不必要的检查和交叉重复检查。检查工作不得收取费用，不得要求被检查单位购买指定品牌或者指定生产、销售单位的产品和服务。

第二十八条 运营者对保护工作部门开展的关键信息基础设施网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的关键信息基础设施网络安全检查工作应当予以配合。

第二十九条 在关键信息基础设施安全保护工作中，国家网信部门和国务院电信主管部门、国务院公安部门等应当根据保护工作部门的需要，及时提供技术支持和协助。

第三十条 网信部门、公安机关、保护工作部门等有关部门，网络安全服务机构及其工作人员对于在关键信息基础设施安全保护工作中获取的信息，只能用于维护网络安全，并严格按照有关法律、行政法规的要求确保信息安全，不得泄露、出售或者非法向他人提供。

第三十二条 国家采取措施，优先保障能源、电信等关键信息基础设施安全运行。

能源、电信行业应当采取措施，为其他行业和领域的关键信息基础设施安全运行提供重点保障。

第三十三条 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。

第三十四条 国家制定和完善关键信息基础设施安全标准，指导、规范关键信息基础设施安全保护工作。

第三十五条 国家采取措施，鼓励网络安全专门人才从事关键信息基础设施安全保护工作；将运营者安全管理人员、安全技术人员培训纳入国家继续教育体系。

第三十六条 国家支持关键信息基础设施安全防护技术创新和产业发展，组织力量实施关键信息基础设施安全技术攻关。

第三十七条 国家加强网络安全服务机构建设和管理，制定管理要求并加强监督指导，不断提升服务机构能力水平，充分发挥其在关键信息基础设施安全保护中的作用。

第三十八条 国家加强网络安全军民融合，军地协同保护关键信息基础设施安全。

第五章 法律责任

第三十九条 运营者有下列情形之一的，由有关主管部门依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处10万元以上100万元以下罚款，对直接负责的主管人员处1万元以上10万元以下罚款：

（一）在关键信息基础设施发生较大变化，可能影响其认定结果时未及时将相关情况报告保护工作部门的；

（二）安全保护措施未与关键信息基础设施同步规划、同步建设、同步使用的；

（三）未建立健全网络安全保护制度和责任制的；

（四）未设置专门安全管理机构的；

（五）未对专门安全管理机构负责人和关键岗位人员进行安全背景审查的；

（六）开展与网络安全和信息化有关的决策没有专门安全管理机构人员参与的；

（七）专门安全管理机构未履行本条例第十五条规定的职责的；

（八）未对关键信息基础设施每年至少进行一次网络安全检测和风险评估，未对发现的安全问题及时整改，或者未按照保护工作部门要求报送情况的；

（九）采购网络产品和服务，未按照国家有关规定与网络产品和服务提供者签订安全保密协议的；

（十）发生合并、分立、解散等情况，未及时报告保护工作部门，或者未按照保护工作部门的要求对关键信息基础设施进行处置的。

第四十条 运营者在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，未按照有关规定向保护工作部门、公安机关报告的，由保护工作部门、公安机关依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处10万元以上100万元以下罚款，对直接负责的主管人员处1万元以上10万元以下罚款。

第四十一条 运营者采购可能影响国家安全的网络产品和服务，未按照国家网络安全规定进行安全审查的，由国家网信部门等有关主管部门依据职责责令改正，处采购金额1倍以上10倍以下罚款，对直接负责的主管人员和其他直接责任人员处1万元以上10万元以下罚款。

第四十二条 运营者对保护工作部门开展的关键信息基础设施网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的关键信息基础设施网络安全检查工作不予配合的，由有关主管部门责令改正；拒不改正的，处5万元以上50万元以下罚款，对直接负责的主管人员和其他直接责任人员处1万元以上10万元以下罚款；情节严重的，依法追究相应法律责任。

第四十三条 实施非法侵入、干扰、破坏关键信息基础设施，危害其安全的活动尚不构成犯罪的，依照《中华人民共和国网络安全法》有关规定，由公安机关没收违法所得，处5日以下拘留，可以并处5万元以上50万元以下罚款；情节较重的，处5日以上15日以下拘留，可以并处10万元以上100万元以下罚款。

单位有前款行为的，由公安机关没收违法所得，处10万元以上100万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本条例第五条第二款和第三十一条规定，受到治安管理处罚的人员，5年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

第四十四条 网信部门、公安机关、保护工作部门和其他有关部门及其工作人员未履行关键信息基础设施安全保护和监督管理职责或者玩忽职守、滥用职权、徇私舞弊的，依法对直接负责的主管人员和其他直接责任人员给予处分。

第四十五条 公安机关、保护工作部门和其他有关部门在开展关键信息基础设施网络安全检查工作中收取费用，或者要求被检查单位购买指定品牌或者指定生产、销售单位的产品和服务的，由其上级机关责令改正，退还收取的费用；情节严重的，依法对直接负责的主管人员和其他直接责任人员给予处分。

第四十六条 网信部门、公安机关、保护工作部门等有关部门、网络安全服务机构及其工作人员将在关键信息基础设施安全保护工作中获取的信息用于其他用途，或者泄露、出售、非法向他人提供的，依法对直接负责的主管人员和其他直接责任人员给予处分。

第四十七条 关键信息基础设施发生重大和特别重大网络安全事件，经调查确定为责任事故的，除应当查明运营者责任并依法予以追究外，还应查明相关网络安全服务机构及有关部门的责任，对有失职、渎职及其他违法行为的，依法追究责任。

第四十八条 电子政务关键信息基础设施的运营者不履行本条例规定的网络安全保护义务的，依照《中华人民共和国网络安全法》有关规定予以处理。

第四十九条 违反本条例规定，给他人造成损害的，依法承担民事责任。

违反本条例规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第六章 附 则

第五十条 存储、处理涉及国家秘密信息的关键信息基础设施的安全保护，还应当遵守保密法律、行政法规的规定。

关键信息基础设施中的密码使用和管理，还应当遵守相关法律、行政法规的规定。

第五十一条 本条例自2021年9月1日起施行。

网络安全审查办法

第一条 为了确保关键信息基础设施供应链安全，保障网络安全和数据安全，维护国家安全，根据《中华人民共和国国家安全法》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《关键信息基础设施安全保护条例》，制定本办法。

第二条 关键信息基础设施运营者采购网络产品和服务，网络平台运营者开展数据处理活动，影响或者可能影响国家安全的，应当按照本办法进行网络安全审查。

前款规定的关键信息基础设施运营者、网络平台运营者统称为当事人。

第三条 网络安全审查坚持防范网络安全风险与促进先进技术应用相结合、过程公正透明与知识产权保护相结合、事前审查与持续监管相结合、企业承诺与社会监督相结合，从产品和服务以及数据处理活动安全性、可能带来的国家安全风险等方面进行审查。

第四条 在中央网络安全和信息化委员会领导下，国家互联网信息办公室会同中华人民共和国国家发展和改革委员会、中华人民共和国工业和信息化部、中华人民共和国公安部、中华人民共和国国家安全部、中华人民共和国财政部、中华人民共和国商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、中国证券监督管理委员会、国家保密局、国家密码管理局建立国家网络安全审查工作机制。

网络安全审查办公室设在国家互联网信息办公室，负责制定网络安全审查相关制度规范，组织网络安全审查。

第五条 关键信息基础设施运营者采购网络产品和服务的，应当预判该产品和服务投入使用后可能带来的国家安全风险。影响或者可能影响国家安全的，应当向网络安全审查办公室申报网络安全审查。

关键信息基础设施安全保护工作部门可以制定本行业、本领域预判指南。

第六条 对于申报网络安全审查的采购活动，关键信息基础设施运营者应当通过采购文件、协议等要求产品和服务提供者配合网络安全审查，包括承诺不利用提供产品和服务的便利条件非法获取用户数据、非法控制和操纵用户设备，无正当理由不中断产品供应或者必要的技术支持服务等。

第七条 掌握超过100万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。

第八条 当事人申报网络安全审查，应当提交以下材料：

（一）申报书；

（二）关于影响或者可能影响国家安全的分析报告；

（三）采购文件、协议、拟签订的合同或者拟提交的首次公开募股（IPO）等上市申请文件；

（四）网络安全审查工作需要的其他材料。

第九条 网络安全审查办公室应当自收到符合本办法第八条规定的审查申报材料起10个工作日内，确定是否需要审查并书面通知当事人。

第十条 网络安全审查重点评估相关对象或者情形的以下国家安全风险因素：

（一）产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或者破坏的风险；

（二）产品和服务供应中断对关键信息基础设施业务连续性的危害；

（三）产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险；

（四）产品和服务提供者遵守中国法律、行政法规、部门规章情况；

（五）核心数据、重要数据或者大量个人信息被窃取、泄露、毁损以及非法利用、非法出境的风险；

（六）上市存在关键信息基础设施、核心数据、重要数据或者大量个人信息被外国政府影响、控制、恶意利用的风险，以及网络信息安全风险；

（七）其他可能危害关键信息基础设施安全、网络安全和数据安全的因素。

第十一条 网络安全审查办公室认为需要开展网络安全审查的，应当自向当事人发出书面通知之日起30个工作日内完成初步审查，包括形成审查结论建议和将审查结论建议发送网络安全审查工作机制成员单位、相关部门征求意见；情况复杂的，可以延长15个工作日。

第十二条 网络安全审查工作机制成员单位和相关部门应当自收到审查结论建议之日起15个工作日内书面回复意见。

网络安全审查工作机制成员单位、相关部门意见一致的，网络安全审查办公室以书面形式将审查结论通知当事人；意见不一致的，按照特别审查程序处理，并通知当事人。

第十三条 按照特别审查程序处理的，网络安全审查办公室应当听取相关单位和部门意见，进行深入分析评估，再次形成审查结论建议，并征求网络安全审查工作机制成员单位和相关部门意见，按程序报中央网络安全和信息化委员会批准后，形成审查结论并书面通知当事人。

第十四条 特别审查程序一般应当在90个工作日内完成，情况复杂的可以延长。

第十五条 网络安全审查办公室要求提供补充材料的，当事人、产品和服务提供者应当予以配合。提交补充材料的时间不计入审查时间。

第十六条 网络安全审查工作机制成员单位认为影响或者可能影响国家安全的网络产品和服务以及数据处理活动，由网络安全审查办公室按程序报中央网络安全和信息化委员会批准后，依照本办法的规定进行审查。

为了防范风险，当事人应当在审查期间按照网络安全审查要求采取预防和消减风险的措施。

第十七条 参与网络安全审查的相关机构和人员应当严格保护知识产权，对在审查工作中知悉的商业秘密、个人信息，当事人、产品和服务提供者提交的未公开材料，以及其他未公开信息承担保密义务；未经信息提供方同意，不得向无关方披露或者用于审查以外的目的。

第十八条 当事人或者网络产品和服务提供者认为审查人员有失客观公正，或者未能对审查工作中知悉的信息承担保密义务的，可以向网络安全审查办公室或者有关部门举报。

第十九条 当事人应当督促产品和服务提供者履行网络安全审查中作出的承诺。

网络安全审查办公室通过接受举报等形式加强事前事中事后监督。

第二十条 当事人违反本办法规定的，依照《中华人民共和国网络安全法》、《中华人民共和国数据安全法》的规定处理。

第二十一条 本办法所称网络产品和服务主要指核心网络设备、重要通信产品、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务，以及其他对关键信息基础设施安全、网络安全和数据安全有重要影响的网络产品和服务。

第二十二条 涉及国家秘密信息的，依照国家有关保密规定执行。

国家对数据安全审查、外商投资安全审查另有规定的，应当同时符合其规定。

第二十三条 本办法自2022年2月15日起施行。2020年4月13日公布的《网络安全审查办法》（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、国家安全部、财政部、商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局令第6号）同时废止。

云计算服务安全评估办法

第一条 为提高党政机关、关键信息基础设施运营者采购使用云计算服务的安全可控水平，制定本办法。

第二条 云计算服务安全评估坚持事前评估与持续监督相结合，保障安全与促进应用相统一，依据有关法律法规和政策规定，参照国家有关网络安全标准，发挥专业技术机构、专家作用，客观评价、严格监督云计算服务平台（以下简称“云平台”）的安全性、可控性，为党政机关、关键信息基础设施运营者采购云计算服务提供参考。

本办法中的云平台包括云计算服务软硬件设施及其相关管理制度等。

第三条 云计算服务安全评估重点评估以下内容：

（一）云平台管理运营者（以下简称“云服务商”）的征信、经营状况等基本情况；

（二）云服务商人员背景及稳定性，特别是能够访问客户数据、能够收集相关元数据的人员；

（三）云平台技术、产品和服务供应链安全情况；

（四）云服务商安全管理能力及云平台安全防护情况；

（五）客户迁移数据的可行性和便捷性；

（六）云服务商的业务连续性；

（七）其他可能影响云服务安全的因素。

第四条 国家互联网信息办公室会同国家发展和改革委员会、工业和信息化部、财政部建立云计算服务安全评估工作协调机制（以下简称“协调机制”），审议云计算服务安全评估政策文件，批准云计算服务安全评估结果，协调处理云计算服务安全评估有关重要事项。

云计算服务安全评估工作协调机制办公室（以下简称“办公室”）设在国家互联网信息办公室网络安全协调局。

第五条 云服务商可申请对面向党政机关、关键信息基础设施提供云计算服务的云平台进行安全评估。

第六条 申请安全评估的云服务商应向办公室提交以下材料：

（一）申报书；

（二）云计算服务系统安全计划；

（三）业务连续性和供应链安全报告；

（四）客户数据可迁移性分析报告；

（五）安全评估工作需要的其他材料。

第七条 办公室受理云服务商申请后，组织专业技术机构参照国家有关标准对云平台进行安全评价。

第八条 专业技术机构应坚持客观、公正、公平的原则，按照国家有关规定，在办公室指导监督下，参照《云计算服务安全指南》《云计算服务安全能力要求》等国家标准，重点评价本办法第三条所述内容，形成评价报告，并对评价结果负责。

第九条 办公室在专业技术机构安全评价基础上，组织云计算服务安全评估专家组进行综合评价。

第十条 云计算服务安全评估专家组根据云服务商申报材料、评价报告等，综合评价云计算服务的安全性、可控性，提出是否通过安全评估的建议。

第十一条 云计算服务安全评估专家组的建议经协调机制审议通过后，办公室按程序报国家互联网信息办公室核准。

云计算服务安全评估结果由办公室发布。

第十二条 云计算服务安全评估结果有效期3年。有效期届满需要延续保持评估结果的，云服务商应在届满前至少6个月向办公室申请复评。

有效期内，云服务商因股权变更、企业重组等导致实控人或控股权发生变化的，应重新申请安全评估。

第十三条 办公室通过组织抽查、接受举报等形式，对通过评估的云平台开展持续监督，重点监督有关安全控制措施有效性、重大变更、应急响应、风险处置等内容。

通过评估的云平台已不再满足要求的，经协调机制审议、国家互联网信息办公室核准后撤销通过评估的结论。

第十四条 通过评估的云平台停止提供服务时，云服务商应至少提前6个月通知客户和办公室，并配合客户做好迁移工作。

第十五条 云服务商对所提供申报材料的真实性负责。在评估过程中拒绝按要求提供材料或故意提供虚假材料的，按评估不通过处理。

第十六条 未经云服务商同意，参与评估工作的相关机构和人员不得披露云服务商提交的未公开材料以及评估工作中获悉的其他非公开信息，不得将云服务商提供的信息用于评估以外的目的。

第十七条 本办法自2019年9月1日起施行。

汽车数据安全管理若干规定（试行）

第一条 为了规范汽车数据处理活动，保护个人、组织的合法权益，维护国家安全和社会公共利益，促进汽车数据合理开发利用，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》等法律、行政法规，制定本规定。

第二条 在中华人民共和国境内开展汽车数据处理活动及其安全监管，应当遵守相关法律、行政法规和本规定的要求。

第三条 本规定所称汽车数据，包括汽车设计、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。

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。

汽车数据处理者，是指开展汽车数据处理活动的组织，包括汽车制造商、零部件和软件供应商、经销商、维修机构以及出行服务企业等。

个人信息，是指以电子或者其他方式记录的与已识别或者可识别的车主、驾驶人、乘车人、车外人员等有关的各种信息，不包括匿名化处理后的信息。

敏感个人信息，是指一旦泄露或者非法使用，可能导致车主、驾驶人、乘车人、车外人员等受到歧视或者人身、财产安全受到严重危害的个人信息，包括车辆行踪轨迹、音频、视频、图像和生物识别特征等信息。

重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益或者个人、组织合法权益的数据，包括：

（一）军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量等数据；

（二）车辆流量、物流等反映经济运行情况的数据；

（三）汽车充电网的运行数据；

（四）包含人脸信息、车牌信息等的车外视频、图像数据；

（五）涉及个人信息主体超过10万人的个人信息；

（六）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确定的其他可能危害国家安全、公共利益或者个人、组织合法权益的数据。

第四条 汽车数据处理者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。

第五条 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。

第六条 国家鼓励汽车数据依法合理有效利用，倡导汽车数据处理者在开展汽车数据处理活动中坚持：

（一）车内处理原则，除非确有必要不向车外提供；

（二）默认不收集原则，除非驾驶人自主设定，每次驾驶时默认设定为不收集状态；

（三）精度范围适用原则，根据所提供功能服务对数据精度的要求确定摄像头、雷达等的覆盖范围、分辨率；

（四）脱敏处理原则，尽可能进行匿名化、去标识化等处理。

第七条 汽车数据处理者处理个人信息应当通过用户手册、车载显示面板、语音、汽车使用相关应用程序等显著方式，告知个人以下事项：

（一）处理个人信息的种类，包括车辆行踪轨迹、驾驶习惯、音频、视频、图像和生物识别特征等；

（二）收集各类个人信息的具体情境以及停止收集的方式和途径；

（三）处理各类个人信息的目的、用途、方式；

（四）个人信息保存地点、保存期限，或者确定保存地点、保存期限的规则；

（五）查阅、复制其个人信息以及删除车内、请求删除已经提供给车外的个人信息的方式和途径；

（六）用户权益事务联系人的姓名和联系方式；

（七）法律、行政法规规定的应当告知的其他事项。

第八条 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。

因保证行车安全需要，无法征得个人同意采集到车外个人信息且向车外提供的，应当进行匿名化处理，包括删除含有能够识别自然人的画面，或者对画面中的人脸信息等进行局部轮廓化处理等。

第九条 汽车数据处理者处理敏感个人信息，应当符合以下要求或者符合法律、行政法规和强制性国家标准等其他要求：

（一）具有直接服务于个人的目的，包括增强行车安全、智能驾驶、导航等；

（二）通过用户手册、车载显示面板、语音以及汽车使用相关应用程序等显著方式告知必要性以及对个人的影响；

（三）应当取得个人单独同意，个人可以自主设定同意期限；

（四）在保证行车安全的前提下，以适当方式提示收集状态，为个人终止收集提供便利；

（五）个人要求删除的，汽车数据处理者应当在十个工作日内删除。

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，方可收集指纹、声纹、人脸、心律等生物识别特征信息。

第十条 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。

风险评估报告应当包括处理的重要数据的种类、数量、范围、保存地点与期限、使用方式，开展数据处理活动情况以及是否向第三方提供，面临的数据安全风险及其应对措施等。

第十一条 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。未列入重要数据的涉及个人信息数据的出境安全管理，适用法律、行政法规的有关规定。

我国缔结或者参加的国际条约、协定有不同规定的，适用该国际条约、协定，但我国声明保留的条款除外。

第十二条 汽车数据处理者向境外提供重要数据，不得超出出境安全评估时明确的目的、范围、方式和数据种类、规模等。

国家网信部门会同国务院有关部门以抽查等方式核验前款规定事项，汽车数据处理者应当予以配合，并以可读等便利方式予以展示。

第十三条 汽车数据处理者开展重要数据处理活动，应当在每年十二月十五日前向省、自治区、直辖市网信部门和有关部门报送以下年度汽车数据安全管理情况：

（一）汽车数据安全管理负责人、用户权益事务联系人的姓名和联系方式；

（二）处理汽车数据的种类、规模、目的和必要性；

（三）汽车数据的安全防护和管理措施，包括保存地点、期限等；

（四）向境内第三方提供汽车数据情况；

（五）汽车数据安全事件和处置情况；

（六）汽车数据相关的用户投诉和处理情况；

（七）国家网信部门会同国务院工业和信息化、公安、交通运输等有关部门明确的其他汽车数据安全管理情况。

第十四条 向境外提供重要数据的汽车数据处理者应当在本规定第十三条要求的基础上，补充报告以下情况：

（一）接收者的基本情况；

（二）出境汽车数据的种类、规模、目的和必要性；

（三）汽车数据在境外的保存地点、期限、范围和方式；

（四）涉及向境外提供汽车数据的用户投诉和处理情况；

（五）国家网信部门会同国务院工业和信息化、公安、交通运输等有关部门明确的向境外提供汽车数据需要报告的其他情况。

第十五条 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，根据处理数据情况对汽车数据处理者进行数据安全评估，汽车数据处理者应当予以配合。

参与安全评估的机构和人员不得披露评估中获悉的汽车数据处理者商业秘密、未公开信息，不得将评估中获悉的信息用于评估以外目的。

第十六条 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。

第十七条 汽车数据处理者开展汽车数据处理活动，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。

开展汽车数据处理活动造成用户合法权益或者公共利益受到损害的，汽车数据处理者应当依法承担相应责任。

第十八条 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《中华人民共和国网络安全法》、《中华人民共和国数据安全法》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。

第十九条 本规定自2021年10月1日起施行。

NETWORK SECURITY

网络安全为人民
网络安全靠人民

—共建网络安全 共享网络文明—

BUILD NETWORK SECURITY AND SHARE NETWORK CIVILIZATION