国家网络安全宣传周
China Cybersecurity Week

9月11日-9月17日
2023年陕西省
第十届国家网络安全宣传周
THE TENTH NATIONAL CYBER SECURITY PUBLICITY WEEK OF SHAANXI PROVINCE

网络安全为人民
网络安全靠人民

主办单位

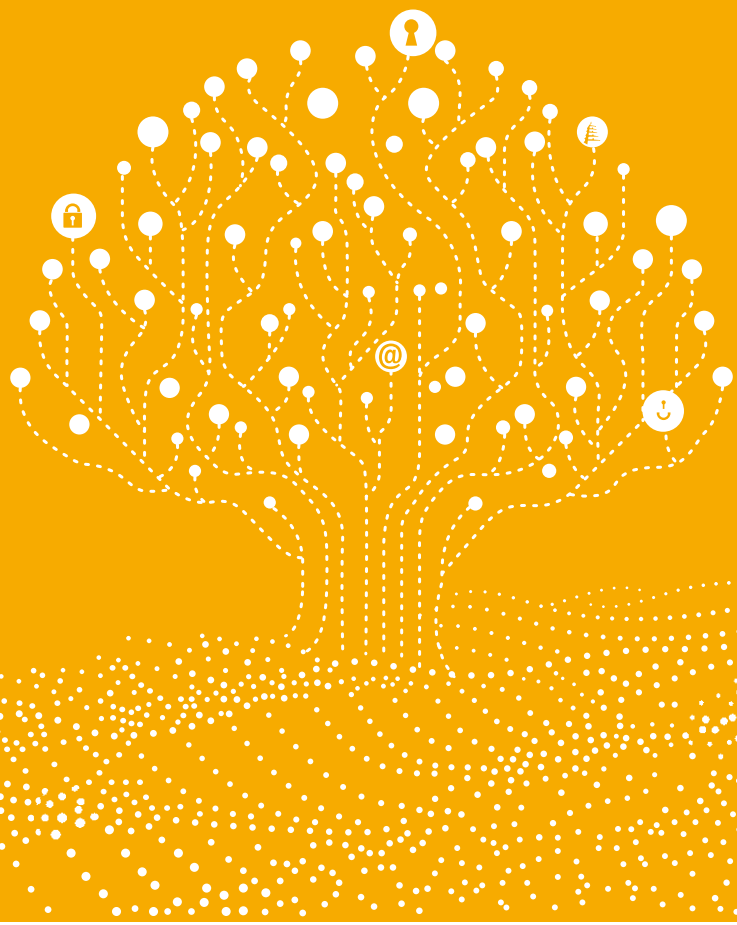
中共陕西省委宣传部、中共陕西省委网信办、陕西省教育厅、
陕西省公安厅、陕西省通信管理局、陕西省总工会、
共青团陕西省委、陕西省妇女联合会、中国人民银行陕西省分行

2023

国家网络安全宣传周

NATIONAL CYBER
SECURITY PUBLICITY WEEK

国家网络安全宣传周
China Cybersecurity Week



前言 FOREWORD

2023年国家网络安全宣传周将于2023年9月11日-17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。陕西省第十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陕西省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。

9月11日-9月17日
2023年陕西省
第十届国家网络安全宣传周
THE TENTH NATIONAL CYBER SECURITY PUBLICITY WEEK OF SHAANXI PROVINCE

中共陕西省委网信办
陕西省互联网信息办公室

ACTIVITY INTRODUCTION

活动介绍

2023年陕西省 第十届国家网络安全宣传周

THE TENTH NATIONAL CYBER SECURITY PUBLICITY WEEK OF SHAANXI PROVINCE

活动时间：

9月11日-9月17日

活动主题：

网络安全为人民 网络安全靠人民

主办单位：

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、
中国人民银行陕西省分行

活动介绍：

开幕式、网络安全博览会、
网络安全技术应用论坛

CATALOGUE

目 录

中华人民共和国反电信网络诈骗法

第一章 总则

第一条 为了预防、遏制和惩治电信网络诈骗活动，加强反电信网络诈骗工作，保护公民和组织的合法权益，维护社会稳定和国家安全，根据宪法，制定本法。

第二条 本法所称电信网络诈骗，是指以非法占有为目的，利用电信网络技术手段，通过远程、非接触等方式，诈骗公私财物的行为。

第三条 打击治理在中华人民共和国境内实施的电信网络诈骗活动或者中华人民共和国公民在境外实施的电信网络诈骗活动，适用本法。境外的组织、个人针对中华人民共和国境内实施电信网络诈骗活动的，或者为他人针对境内实施电信网络诈骗活动提供产品、服务等帮助的，依照本法有关规定处理和追究责任。

第四条 反电信网络诈骗工作坚持以人民为中心，统筹发展和安全；坚持系统观念、法治思维，注重源头治理、综合治理；坚持齐抓共管、群防群治，全面落实打防管控各项措施，加强社会宣传教育防范；坚持精准防治，保障正常生产经营活动和群众生活便利。

第五条 反电信网络诈骗工作应当依法进行，维护公民和组织的合法权益。

有关部门和单位、个人应当对在反电信网络诈骗工作过程中知悉的国家秘密、商业秘密和个人隐私、个人信息予以保密。

第六条 国务院建立反电信网络诈骗工作机制，统筹协调打击治理工作。

地方各级人民政府组织领导本行政区域内反电信网络诈骗工作，确定反电信网络诈骗目标任务和工作机制，开展综合治理。

公安机关牵头负责反电信网络诈骗工作，金融、电信、网信、市场监管等有关部门依照职责履行监管主体责任，负责本行业领域反电信网络诈骗工作。人民法院、人民检察院发挥审判、检察职能作用，依法防范、惩治电信网络诈骗活动。

电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者承担风险防控责任，建立反电信网络诈骗内部控制机制和安全责任制度，加强新业务涉诈风险安全评估。

第七条 有关部门、单位在反电信网络诈骗工作中应当密切协作，实现跨行业、跨地域协同配合、快速联动，加强专业队伍建设，有效打击治理电信网络诈骗活动。

第八条 各级人民政府和有关部门应当加强反电信网络诈骗宣传，普及相关法律和知识，提高公众对各类电信网络诈骗方式的防骗意识和识骗能力。

教育行政、市场监管、民政等有关部门和村民委员会、居民委员会，应当结合电信网络诈骗受害群体的分布等特征，加强对老年人、青少年等群体的宣传教育，增强反电信网络诈骗宣传教育的针对性、精准性，开展反电信网络诈骗宣传教育进学校、进企业、进社区、进农村、进家庭等活动。

各单位应当加强内部防范电信网络诈骗工作，对工作人员开展防范电信网络诈骗教育；个人应当加强电信网络诈骗防范意识。单位、个人应当协助、配合有关部门依照本法规定开展反电信网络诈骗工作。

第二章 电信治理

第九条 电信业务经营者应当依法全面落实电话用户真实身份信息登记制度。

基础电信企业和移动通信转售企业应当承担对代理商落实电话用户实名制管理责任，在协议中明确代理商实名制登记的责任和有关违约处置措施。

第十条 办理电话卡不得超出国家有关规定限制的数量。

对经识别存在异常办卡情形的，电信业务经营者有权加强核查或者拒绝办卡。具体识别办法由国务院电信主管部门制定。

国务院电信主管部门组织建立电话用户开卡数量核验机制和风险信息共享机制，并为用户查询名下电话卡信息提供便捷渠道。

第十一条 电信业务经营者对监测识别的涉诈异常电话卡用户应当重新进行实名核验，根据风险等级采取有区别的、相应的核验措施。对未按规定核验或者核验未通过的，电信业务经营者可以限制、暂停有关电话卡功能。

第十二条 电信业务经营者建立物联网卡用户风险评估制度，评估未通过的，不得向其销售物联网卡；严格登记物联网卡用户身份信息；采取有效技术措施限定物联网卡开通功能、使用场景和适用设备。

单位用户从电信业务经营者购买物联网卡再将载有物联网卡的设备销售给其他用户的，应当核验和登记用户身份信息，并将销量、存量及用户实名信息传送给号码归属的电信业务经营者。

电信业务经营者对物联网卡的使用建立监测预警机制。对存在异常使用情形的，应当采取暂停服务、重新核验身份和使用场景或者其他合同约定的处置措施。

第十三条 电信业务经营者应当规范真实主叫号码传送和电信线路出租，对改号电话进行封堵拦截和溯源核查。

电信业务经营者应当严格规范国际通信业务出入口局主叫号码传送，真实、准确向用户提示来电号码所属国家或者地区，对网内和网间虚假主叫、不规范主叫进行识别、拦截。

第十四条 任何单位和个人不得非法制造、买卖、提供或者使用下列设备、软件：

（一）电话卡批量插入设备；

（二）具有改变主叫号码、虚拟拨号、互联网电话违规接入公用电信网络等功能的设备、软件；

（三）批量账号、网络地址自动切换系统，批量接收提供短信验证、语音验证的平台；

（四）其他用于实施电信网络诈骗等违法犯罪的设备、软件。

电信业务经营者、互联网服务提供者应当采取技术措施，及时识别、阻断前款规定的非法设备、软件接入网络，并向公安机关和相关行业主管部门报告。

第三章 金融治理

第十五条 银行业金融机构、非银行支付机构为客户开立银行账户、支付账户及提供支付结算服务，和与客户业务关系存续期间，应当建立客户尽职调查制度，依法识别受益所有人，采取相应风险管理措施，防范银行账户、支付账户等被用于电信网络诈骗活动。

第十六条 开立银行账户、支付账户不得超出国家有关规定限制的数量。

对经识别存在异常开户情形的，银行业金融机构、非银行支付机构有权加强核查或者拒绝开户。

中国人民银行、国务院银行业监督管理机构组织有关清算机构建立跨机构开户数量核验机制和风险信息共享机制，并为客户提供查询名下银行账户、支付账户的便捷渠道。银行业金融机构、非银行支付机构应当按照国家有关规定提供开户情况和有关风险信息。相关信息不得用于反电信网络诈骗以外的其他用途。

第十七条 银行业金融机构、非银行支付机构应当建立开立企业账户异常情形的风险防控机制。金融、电信、市场监管、税务等有关部门建立开立企业账户相关信息共享查询系统，提供联网核查服务。

市场主体登记机关应当依法对企业实名登记履行身份信息核验职责；依照规定对登记事项进行监督检查，对可能存在虚假登记、涉诈异常的企业重点监督检查，依法撤销登记的，依照前款的规定及时共享信息；为银行业金融机构、非银行支付机构进行客户尽职调查和依法识别受益所有人提供便利。

第十八条 银行业金融机构、非银行支付机构应当对银行账户、支付账户及支付结算服务加强监测，建立完善符合电信网络诈骗活动特征的异常账户和可疑交易监测机制。

中国人民银行统筹建立跨银行业金融机构、非银行支付机构的反洗钱统一监测系统，会同国务院公安部门完善与电信网络诈骗犯罪资金流转特点相适应的反洗钱可疑交易报告制度。

对监测识别的异常账户和可疑交易，银行业金融机构、非银行支付机构应当根据风险情况，采取核实交易情况、重新核验身份、延迟支付结算、限制或者中止有关业务等必要的防范措施。

银行业金融机构、非银行支付机构依照第一款规定开展异常账户和可疑交易监测时，可以收集异常客户互联网协议地址、网卡地址、支付受理终端信息等必要的交易信息、设备位置信息。上述信息未经客户授权，不得用于反电信网络诈骗以外的其他用途。

第十九条 银行业金融机构、非银行支付机构应当按照国家有关规定，完整、准确传输直接提供商品或者服务的商户名称、收付款客户名称及账号等交易信息，保证交易信息的真实、完整和支付全流程中的一致性。

第二十条 国务院公安部门会同有关部门建立完善电信网络诈骗涉案资金即时查询、紧急止付、快速冻结、及时解冻和资金返还制度，明确有关条件、程序和救济措施。

公安机关依法决定采取上述措施的，银行业金融机构、非银行支付机构应当予以配合。

第四章 互联网治理

第二十一条 电信业务经营者、互联网服务提供者为用户提供下列服务，在与用户签订协议或者确认提供服务时，应当依法要求用户提供真实身份信息，用户不提供真实身份信息的，不得提供服务：

（一）提供互联网接入服务；

（二）提供网络代理等网络地址转换服务；

（三）提供互联网域名注册、服务器托管、空间租用、云服务、内容分发服务；

（四）提供信息、软件发布服务，或者提供即时通讯、网络交易、网络游戏、网络直播发布、广告推广服务。

第二十二条 互联网服务提供者对监测识别的涉诈异常账号应当重新核验，根据国家有关规定采取限制功能、暂停服务等处置措施。

互联网服务提供者应当根据公安机关、电信主管部门要求，对涉案电话卡、涉诈异常电话卡所关联注册的有关互联网账号进行核验，根据风险情况，采取限期改正、限制功能、暂停使用、关闭账号、禁止重新注册等处置措施。

第二十三条 设立移动互联网应用程序应当按照国家有关规定向电信主管部门办理许可或者备案手续。

为应用程序提供封装、分发服务的，应当登记并核验应用程序开发运营者的真实身份信息，核验应用程序的功能、用途。

公安、电信、网信等部门和电信业务经营者、互联网服务提供者应当加强对分发平台以外途径下载传播的涉诈应用程序重点监测、及时处置。

第二十四条 提供域名解析、域名跳转、网址链接转换服务的，应当按照国家有关规定，核验域名注册、解析信息和互联网协议地址的真实性、准确性，规范域名跳转，记录并留存所提供相应服务的日志信息，支持实现对解析、跳转、转换记录的溯源。

第二十五条 任何单位和个人不得为他人实施电信网络诈骗活动提供下列支持或者帮助：

（一）出售、提供个人信息；

（二）帮助他人通过虚拟货币交易等方式洗钱；

（三）其他为电信网络诈骗活动提供支持或者帮助的行为。

电信业务经营者、互联网服务提供者应当依照国家有关规定，履行合理注意义务，对利用下列业务从事涉诈支持、帮助活动进行监测识别和处置：

（一）提供互联网接入、服务器托管、网络存储、通讯传输、线路出租、域名解析等网络资源服务；

（二）提供信息发布或者搜索、广告推广、引流推广等网络推广服务；

（三）提供应用程序、网站等网络技术、产品的制作、维护服务；

（四）提供支付结算服务。

第二十六条 公安机关办理电信网络诈骗案件依法调取证据的，互联网服务提供者应当及时提供技术支持和协助。

互联网服务提供者依照本法规定对有关涉诈信息、活动进行监测时，发现涉诈违法犯罪线索、风险信息的，应当依照国家有关规定，根据涉诈风险类型、程度情况移送公安、金融、电信、网信等部门。有关部门应当建立完善反馈机制，将相关情况及时告知移送单位。

第五章 综合措施

第二十七条 公安机关应当建立完善打击治理电信网络诈骗工作机制，加强专门队伍和专业技术建设，各警种、各地公安机关应当密切配合，依法有效惩处电信网络诈骗活动。

公安机关接到电信网络诈骗活动的报案或者发现电信网络诈骗活动，应当依照《中华人民共和国刑事诉讼法》的规定立案侦查。

第二十八条 金融、电信、网信部门依照职责对银行业金融机构、非银行支付机构、电信业务经营者、互联网服务提供者落实本法规定情况进行监督检查。有关监督检查活动应当依法规范开展。

第二十九条 个人信息处理者应当依照《中华人民共和国个人信息保护法》等法律规定，规范个人信息处理，加强个人信息保护，建立个人信息被用于电信网络诈骗的防范机制。

履行个人信息保护职责的部门、单位对可能被电信网络诈骗利用的物流信息、交易信息、贷款信息、医疗信息、婚介信息等实施重点保护。公安机关办理电信网络诈骗案件，应当同时查证犯罪所利用的个人信息来源，依法追究相关人员和单位责任。

第三十条 电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者应当对从业人员和用户开展反电信网络诈骗宣传，在有关业务活动中对防范电信网络诈骗作出提示，对本领域新出现的电信网络诈骗手段及时向用户作出提醒，对非法买卖、出租、出借本人有关卡、账户、账号等被用于电信网络诈骗的法律责任作出警示。

新闻、广播、电视、文化、互联网信息服务等单位，应当面向社会有针对性地开展反电信网络诈骗宣传教育。

任何单位和个人有权举报电信网络诈骗活动，有关部门应当依法及时处理，对提供有效信息的举报人依照规定给予奖励和保护。

第三十一条 任何单位和个人不得非法买卖、出租、出借电话卡、物联网卡、电信线路、短信端口、银行账户、支付账户、互联网账号等，不得提供实名核验帮助；不得假冒他人身份或者虚构代理关系开立上述卡、账户、账号等。

对经设区的市级以上公安机关认定的实施前款行为的单位、个人和相关组织者，以及因从事电信网络诈骗活动或者关联犯罪受过刑事处罚的人员，可以按照国家有关规定记入信用记录，采取限制其有关卡、账户、账号等功能和停止非柜面业务、暂停新业务、限制入网等措施。对上述认定和措施有异议的，可以提出申诉，有关部门应当建立健全申诉渠道、信用修复和救济制度。具体办法由国务院公安部门会同有关主管部门规定。

第三十二条 国家支持电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者研究开发有关电信网络诈骗反制技术，用于监测识别、动态封堵和处置涉诈异常信息、活动。

国务院公安部门、金融管理部门、电信主管部门和国家网信部门等应当统筹负责本行业领域反制技术措施建设，推进涉电信网络诈骗样本信息数据共享，加强涉诈用户信息交叉核验，建立有关涉诈异常信息、活动的监测识别、动态封堵和处置机制。

依据本法第十一条、第十二条、第十八条、第二十二条和前款规定，对涉诈异常情形采取限制、暂停服务等处置措施的，应当告知处置原因、救济渠道及需要提交的资料等事项，被处置对象可以向作出决定或者采取措施的部门、单位提出申诉。作出决定的部门、单位应当建立完善申诉渠道，及时受理申诉并核查，核查通过的，应当即时解除有关措施。

第三十三条 国家推进网络身份认证公共服务建设，支持个人、企业自愿使用，电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者对存在涉诈异常的电话卡、银行账户、支付账户、互联网账号，可以通过国家网络身份认证公共服务对用户身份重新进行核验。

第三十四条 公安机关应当会同金融、电信、网信部门组织银行业金融机构、非银行支付机构、电信业务经营者、互联网服务提供者等建立预警劝阻系统，对预警发现的潜在被害人，根据情况及时采取相应劝阻措施。对电信网络诈骗案件应当加强追赃挽损，完善涉案资金处置制度，及时返还被害人的合法财产。对遭受重大生活困难的被害人，符合国家有关救助条件的，有关方面依照规定给予救助。

第三十五条 经国务院反电信网络诈骗工作机制决定或者批准，公安、金融、电信等部门对电信网络诈骗活动严重的特定地区，可以依照国家有关规定采取必要的临时风险防范措施。

第三十六条 对前往电信网络诈骗活动严重地区的人员，出境活动存在重大涉电信网络诈骗活动嫌疑的，移民管理机构可以决定不准其出境。

因从事电信网络诈骗活动受过刑事处罚的人员，设区的市级以上公安机关可以根据犯罪情况和预防再犯罪的需要，决定自处罚完毕之日起六个月至三年以内不准其出境，并通知移民管理机构执行。

第三十七条 国务院公安部门等会同外交部门加强国际执法司法合作，与有关国家、地区、国际组织建立有效合作机制，通过开展国际警务合作等方式，提升在信息交流、调查取证、侦查抓捕、追赃挽损等方面的合作水平，有效打击遏制跨境电信网络诈骗活动。

第六章 法律责任

第三十八条 组织、策划、实施、参与电信网络诈骗活动或者为电信网络诈骗活动提供帮助，构成犯罪的，依法追究刑事责任。

前款行为尚不构成犯罪的，由公安机关处十日以上十五日以下拘留；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一万元的，处十万元以下罚款。

第三十九条 电信业务经营者违反本法规定，有下列情形之一的，由有关主管部门责令改正，情节较轻的，给予警告、通报批评，或者处五万元以上五十万元以下罚款；情节严重的，处五十万元以上五百万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对其直接负责的主管人员和其他直接责任人员，处一万元以上二十万元以下罚款：

（一）未落实国家有关规定确定的反电信网络诈骗内部控制机制的；

（二）未履行电话卡、物联网卡实名制登记职责的；

（三）未履行对电话卡、物联网卡的监测识别、监测预警和相关处置职责的；

（四）未对物联网卡用户进行风险评估，或者未限定物联网卡的开通功能、使用场景和适用设备的；

（五）未采取措施对改号电话、虚假主叫或者具有相应功能的非法设备进行监测处置的。

第四十条 银行业金融机构、非银行支付机构违反本法规定，有下列情形之一的，由有关主管部门责令改正，情节较轻的，给予警告、通报批评，或者处五万元以上五十万元以下罚款；情节严重的，处五十万元以上五百万元以下罚款，并可以由有关主管部门责令停止新增业务、缩减业务类型或者业务范围、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，对其直接负责的主管人员和其他直接责任人员，处一万元以上二十万元以下罚款：

（一）未落实国家有关规定确定的反电信网络诈骗内部控制机制的；

（二）未履行尽职调查义务和有关风险管理措施的；

（三）未履行对异常账户、可疑交易的风险监测和相关处置义务的；

（四）未按照规定完整、准确传输有关交易信息的。

第四十一条 电信业务经营者、互联网服务提供者违反本法规定，有下列情形之一的，由有关主管部门责令改正，情节较轻的，给予警告、通报批评，或者处五万元以上五十万元以下罚款；情节严重的，处五十万元以上五百万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对其直接负责的主管人员和其他直接责任人员，处一万元以上二十万元以下罚款：

（一）未落实国家有关规定确定的反电信网络诈骗内部控制机制的；

（二）未履行网络服务实名制职责，或者未对涉案、涉诈电话卡关联注册互联网账号进行核验的；

（三）未按照国家有关规定，核验域名注册、解析信息和互联网协议地址的真实性、准确性，规范域名跳转，或者记录并留存所提供相应服务的日志信息的；

（四）未登记核验移动互联网应用程序开发运营者的真实身份信息或者未核验应用程序的功能、用途，为其提供应用程序封装、分发服务的；

（五）未履行对涉诈互联网账号和应用程序，以及其他电信网络诈骗信息、活动的监测识别和处置义务的；

（六）拒不依法为查处电信网络诈骗犯罪提供技术支持和协助，或者未按规定移送有关违法犯罪线索、风险信息的。

第四十二条 违反本法第十四条、第二十五条第一款规定的，没收违法所得，由公安机关或者有关主管部门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五万元的，处五十万元以下罚款；情节严重的，由公安机关并处十五日以下拘留。

第四十三条 违反本法第二十五条第二款规定，由有关主管部门责令改正，情节较轻的，给予警告、通报批评，或者处五万元以上五十万元以下罚款；情节严重的，处五十万元以上五百万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站或者应用程序，对其直接负责的主管人员和其他直接责任人员，处一万元以上二十万元以下罚款。

第四十四条 违反本法第三十一条第一款规定的，没收违法所得，由公安机关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二万元的，处二十万元以下罚款；情节严重的，并处十五日以下拘留。

第四十五条 反电信网络诈骗工作有关部门、单位的工作人员滥用职权、玩忽职守、徇私舞弊，或者有其他违反本法规定行为，构成犯罪的，依法追究刑事责任。

第四十六条 组织、策划、实施、参与电信网络诈骗活动或者为电信网络诈骗活动提供相关帮助的违法犯罪人员，除依法承担刑事责任、行政责任以外，造成他人损害的，依照《中华人民共和国民法典》等法律的规定承担民事责任。

电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者等违反本法规定，造成他人损害的，依照《中华人民共和国民法典》等法律的规定承担民事责任。

第四十七条 人民检察院在履行反电信网络诈骗职责中，对于侵害国家利益和社会公共利益的行为，可以依法向人民法院提起公益诉讼。

第四十八条 有关单位和个人对依照本法作出的行政处罚和行政强制措施决定不服的，可以依法申请行政复议或者提起行政诉讼。

第七章 附则

第四十九条 反电信网络诈骗工作涉及的有关管理和责任制度，本法没有规定的，适用《中华人民共和国网络安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国反洗钱法》等相关法律规定。

第五十条 本法自2022年12月1日起施行。

生成式人工智能服务管理暂行办法

《生成式人工智能服务管理暂行办法》已经2023年5月23日国家互联网信息办公室2023年第12次室务会会议审议通过，并经国家发展和改革委员会、教育部、科学技术部、工业和信息化部、公安部、国家广播电视总局同意，现予公布，自2023年8月15日起施行。

第一章　总则

第一条 为了促进生成式人工智能健康发展和规范应用，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，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》、《中华人民共和国个人信息保护法》、《中华人民共和国科学技术进步法》等法律、行政法规，制定本办法。

第二条 利用生成式人工智能技术向中华人民共和国境内公众提供生成文本、图片、音频、视频等内容的服务（以下称生成式人工智能服务），适用本办法。

国家对利用生成式人工智能服务从事新闻出版、影视制作、文艺创作等活动另有规定的，从其规定。

行业组织、企业、教育和科研机构、公共文化机构、有关专业机构等研发、应用生成式人工智能技术，未向境内公众提供生成式人工智能服务的，不适用本办法的规定。

第三条 国家坚持发展和安全并重、促进创新和依法治理相结合的原则，采取有效措施鼓励生成式人工智能创新发展，对生成式人工智能服务实行包容审慎和分类分级监管。

第四条 提供和使用生成式人工智能服务，应当遵守法律、行政法规，尊重社会公德和伦理道德，遵守以下规定：

（一）坚持社会主义核心价值观，不得生成煽动颠覆国家政权、推翻社会主义制度，危害国家安全和利益、损害国家形象，煽动分裂国家、破坏国家统一和社会稳定，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，暴力、淫秽色情，以及虚假有害信息等法律、行政法规禁止的内容；

（二）在算法设计、训练数据选择、模型生成和优化、提供服务等过程中，采取有效措施防止产生民族、信仰、国别、地域、性别、年龄、职业、健康等歧视；

（三）尊重知识产权、商业道德，保守商业秘密，不得利用算法、数据、平台等优势，实施垄断和不正当竞争行为；

（四）尊重他人合法权益，不得危害他人身心健康，不得侵害他人肖像权、名誉权、荣誉权、隐私权和个人信息权益；

（五）基于服务类型特点，采取有效措施，提升生成式人工智能服务的透明度，提高生成内容的准确性和可靠性。

第二章　技术发展与治理

第五条 鼓励生成式人工智能技术在各行业、各领域的创新应用，生成积极健康、向上向善的优质内容，探索优化应用场景，构建应用生态体系。

支持行业组织、企业、教育和科研机构、公共文化机构、有关专业机构等在生成式人工智能技术创新、数据资源建设、转化应用、风险防范等方面开展协作。

第六条 鼓励生成式人工智能算法、框架、芯片及配套软件平台等基础技术的自主创新，平等互利开展国际交流与合作，参与生成式人工智能相关国际规则制定。

推动生成式人工智能基础设施和公共训练数据资源平台建设。促进算力资源协同共享，提升算力资源利用效能。推动公共数据分类分级有序开放，扩展高质量的公共训练数据资源。鼓励采用安全可信的芯片、软件、工具、算力和数据资源。

第七条 生成式人工智能服务提供者（以下称提供者）应当依法开展预训练、优化训练等训练数据处理活动，遵守以下规定：

（一）使用具有合法来源的数据和基础模型；

（二）涉及知识产权的，不得侵害他人依法享有的知识产权；

（三）涉及个人信息的，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；

（四）采取有效措施提高训练数据质量，增强训练数据的真实性、准确性、客观性、多样性；

（五）《中华人民共和国网络安全法》、《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》等法律、行政法规的其他有关规定和有关主管部门的相关监管要求。

第八条 在生成式人工智能技术研发过程中进行数据标注的，提供者应当制定符合本办法要求的清晰、具体、可操作的标注规则；开展数据标注质量评估，抽样核验标注内容的准确性；对标注人员进行必要培训，提升尊法守法意识，监督指导标注人员规范开展标注工作。

第三章　服务规范

第九条 提供者应当依法承担网络信息内容生产者责任，履行网络信息安全义务。涉及个人信息的，依法承担个人信息处理者责任，履行个人信息保护义务。

提供者应当与注册其服务的生成式人工智能服务使用者（以下称使用者）签订服务协议，明确双方权利义务。

第十条 提供者应当明确并公开其服务的适用人群、场合、用途，指导使用者科学理性认识和依法使用生成式人工智能技术，采取有效措施防范未成年人用户过度依赖或者沉迷生成式人工智能服务。

第十一条 提供者对使用者的输入信息和使用记录应当依法履行保护义务，不得收集非必要个人信息，不得非法留存能够识别使用者身份的输入信息和使用记录，不得非法向他人提供使用者的输入信息和使用记录。

提供者应当依法及时受理和处理个人关于查阅、复制、更正、补充、删除其个人信息等的请求。

第十二条 提供者应当按照《互联网信息服务深度合成管理规定》对图片、视频等生成内容进行标识。

第十三条 提供者应当在其服务过程中，提供安全、稳定、持续的服务，保障用户正常使用。

第十四条 提供者发现违法内容的，应当及时采取停止生成、停止传输、消除等处置措施，采取模型优化训练等措施进行整改，并向有关主管部门报告。

提供者发现使用者利用生成式人工智能服务从事违法活动的，应当依法依约采取警示、限制功能、暂停或者终止向其提供服务等处置措施，保存有关记录，并向有关主管部门报告。

第十五条 提供者应当建立健全投诉、举报机制，设置便捷的投诉、举报入口，公布处理流程和反馈时限，及时受理、处理公众投诉举报并反馈处理结果。

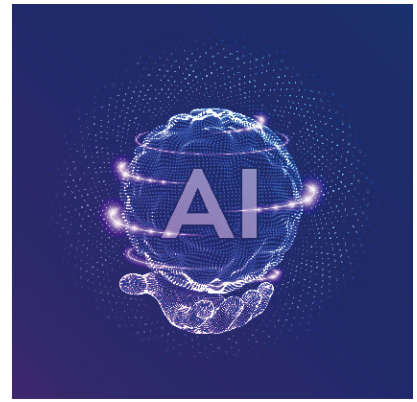
第四章　监督检查和法律责任

第十六条 网信、发展改革、教育、科技、工业和信息化、公安、广播电视、新闻出版等部门，依据各自职责依法加强对生成式人工智能服务的管理。

国家有关主管部门针对生成式人工智能技术特点及其在有关行业和领域的服务应用，完善与创新发展相适应的科学监管方式，制定相应的分类分级监管规则或者指引。

第十七条 提供具有舆论属性或者社会动员能力的生成式人工智能服务的，应当按照国家有关规定开展安全评估，并按照《互联网信息服务算法推荐管理规定》履行算法备案和变更、注销备案手续。

第十八条 使用者发现生成式人工智能服务不符合法律、行政法规和本办法规定的，有权向有关主管部门投诉、举报。



第十九条 有关主管部门依据职责对生成式人工智能服务开展监督检查，提供者应当依法予以配合，按要求对训练数据来源、规模、类型、标注规则、算法机制机理等予以说明，并提供必要的技术、数据等支持和协助。

参与生成式人工智能服务安全评估和监督检查的相关机构和人员对在履行职责中知悉的国家秘密、商业秘密、个人隐私和个人信息应当依法予以保密，不得泄露或者非法向他人提供。

第二十条 对来源于中华人民共和国境外向境内提供生成式人工智能服务不符合法律、行政法规和本办法规定的，国家网信部门应当通知有关机构采取技术措施和其他必要措施予以处置。

第二十一条 提供者违反本办法规定的，由有关主管部门依照《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国科学技术进步法》等法律、行政法规的规定予以处罚；法律、行政法规没有规定的，由有关主管部门依据职责予以警告、通报批评，责令限期改正；拒不改正或者情节严重的，责令暂停提供相关服务。

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。

第五章　附　则

第二十二条 本办法下列用语的含义是：

（一）生成式人工智能技术，是指具有文本、图片、音频、视频等内容生成能力的模型及相关技术。

（二）生成式人工智能服务提供者，是指利用生成式人工智能技术提供生成式人工智能服务（包括通过提供可编程接口等方式提供生成式人工智能服务）的组织、个人。

（三）生成式人工智能服务使用者，是指使用生成式人工智能服务生成内容的组织、个人。

第二十三条 法律、行政法规规定提供生成式人工智能服务应当取得相关行政许可的，提供者应当依法取得许可。

外商投资生成式人工智能服务，应当符合外商投资相关法律、行政法规的规定。

第二十四条 本办法自2023年8月15日起施行。

个人信息出境标准合同办法

《个人信息出境标准合同办法》已经2023年2月3日国家互联网信息办公室2023年第2次室务会议审议通过，现予公布，自2023年6月1日起施行。

第一条 为了保护个人信息权益，规范个人信息出境活动，根据《中华人民共和国个人信息保护法》等法律法规，制定本办法。

第二条 个人信息处理者通过与境外接收方订立个人信息出境标准合同（以下简称标准合同）的方式向中华人民共和国境外提供个人信息，适用本办法。

第三条 通过订立标准合同的方式开展个人信息出境活动，应当坚持自主缔约与备案管理相结合、保护权益与防范风险相结合，保障个人信息跨境安全、自由流动。

第四条 个人信息处理者通过订立标准合同的方式向境外提供个人信息的，应当同时符合下列情形：

（一）非关键信息基础设施运营者；

（二）处理个人信息不满100万人的；

（三）自上年1月1日起累计向境外提供个人信息不满10万人的；

（四）自上年1月1日起累计向境外提供敏感个人信息不满1万人的。

法律、行政法规或者国家网信部门另有规定的，从其规定。

个人信息处理者不得采取数量拆分等手段，将依法应当通过出境安全评估的个人信息通过订立标准合同的方式向境外提供。

第五条 个人信息处理者向境外提供个人信息前，应当开展个人信息保护影响评估，重点评估以下内容：

（一）个人信息处理者和境外接收方处理个人信息的目的、范围、方式等的合法性、正当性、必要性；

（二）出境个人信息的规模、范围、种类、敏感程度，个人信息出境可能对个人信息权益带来的风险；

（三）境外接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障出境个人信息的安全；

（四）个人信息出境后遭到篡改、破坏、泄露、丢失、非法利用等的风险，个人信息权益维护的渠道是否通畅等；

（五）境外接收方所在国家或者地区的个人信息保护政策和法规对标准合同履行的影响；

（六）其他可能影响个人信息出境安全的事项。

第六条 标准合同应当严格按照本办法附件订立。国家网信部门可以根据实际情况对附件进行调整。

个人信息处理者可以与境外接收方约定其他条款，但不得与标准合同相冲突。

标准合同生效后方可开展个人信息出境活动。

第七条 个人信息处理者应当在标准合同生效之日起10个工作日内向所在地省级网信部门备案。备案应当提交以下材料：

（一）标准合同；

（二）个人信息保护影响评估报告。

个人信息处理者应当对所备案材料的真实性负责。

第八条 在标准合同有效期内出现下列情形之一的，个人信息处理者应当重新开展个人信息保护影响评估，补充或者重新订立标准合同，并履行相应备案手续：

（一）向境外提供个人信息的目的、范围、种类、敏感程度、方式、保存地点或者境外接收方处理个人信息的用途、方式发生变化，或者延长个人信息境外保存期限的；

（二）境外接收方所在国家或者地区的个人信息保护政策和法规发生变化等可能影响个人信息权益的；

（三）可能影响个人信息权益的其他情形。

第九条 网信部门及其工作人员对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等应当依法予以保密，不得泄露或者非法向他人提供、非法使用。

第十条 任何组织和个人发现个人信息处理者违反本办法向境外提供个人信息的，可以向省级以上网信部门举报。

第十一条 省级以上网信部门发现个人信息出境活动存在较大风险或者发生个人信息安全事件的，可以依法对个人信息处理者进行约谈。个人信息处理者应当按照要求整改，消除隐患。

第十二条 违反本办法规定的，依据《中华人民共和国个人信息保护法》等法律法规处理；构成犯罪的，依法追究刑事责任。

第十三条 本办法自2023年6月1日起施行。本办法施行前已经开展的个人信息出境活动，不符合本办法规定的，应当自本办法施行之日起6个月内完成整改。

01
法律法规

数据出境安全评估办法

《数据出境安全评估办法》已经2022年5月19日国家互联网信息办公室2022年第10次室务会议审议通过，现予公布，自2022年9月1日起施行。

第一条 为了规范数据出境活动，保护个人信息权益，维护国家安全和社会公共利益，促进数据跨境安全、自由流动，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》、《中华人民共和国个人信息保护法》等法律法规，制定本办法。

第二条 数据处理者向境外提供在中华人民共和国境内运营中收集和产生的重要数据和个人信息的安全评估，适用本办法。法律、行政法规另有规定的，依照其规定。

第三条 数据出境安全评估坚持事前评估和持续监督相结合、风险自评估与安全评估相结合，防范数据出境安全风险，保障数据依法有序自由流动。

第四条 数据处理者向境外提供数据，有下列情形之一的，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估：

（一）数据处理者向境外提供重要数据；

（二）关键信息基础设施运营者和处理100万人以上个人信息的数据处理者向境外提供个人信息；

（三）自上年1月1日起累计向境外提供10万人个人信息或者1万人敏感个人信息的数据处理者向境外提供个人信息；

（四）国家网信部门规定的其他需要申报数据出境安全评估的情形。

第五条 数据处理者在申报数据出境安全评估前，应当开展数据出境风险自评估，重点评估以下事项：

（一）数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性；

（二）出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；

（三）境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；

（四）数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等；

（五）与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等（以下统称法律文件）是否充分约定了数据安全保护责任义务；

（六）其他可能影响数据出境安全的事项。

第六条 申报数据出境安全评估，应当提交以下材料：

（一）申报书；

（二）数据出境风险自评估报告；

（三）数据处理者与境外接收方拟订立的法律文件；

（四）安全评估工作需要的其他材料。

第七条 省级网信部门应当自收到申报材料之日起5个工作日内完成完备性查验。申报材料齐全的，将申报材料报送国家网信部门；申报材料不齐全的，应当退回数据处理者并一次性告知需要补充的材料。

国家网信部门应当自收到申报材料之日起7个工作日内，确定是否受理并书面通知数据处理者。

第八条 数据出境安全评估重点评估数据出境活动可能对国家安全、公共利益、个人或者组织合法权益带来的风险，主要包括以下事项：

（一）数据出境的目的、范围、方式等的合法性、正当性、必要性；

（二）境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境

数据安全的影响；境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求；

（三）出境数据的规模、范围、种类、敏感程度，出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险；

（四）数据安全和个人信息权益是否能够得到充分有效保障；

（五）数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务；

（六）遵守中国法律、行政法规、部门规章情况；

（七）国家网信部门认为需要评估的其他事项。

第九条 数据处理者应当在与境外接收方订立的法律文件中明确约定数据安全保护责任义务，至少包括以下内容：

（一）数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等；

（二）数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施；

（三）对于境外接收方将出境数据再转移给其他组织、个人的约束性要求；

（四）境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形导致难以保障数据安全时，应当采取的安全措施；

（五）违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式；

（六）出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等风险时，妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式。

第十条 国家网信部门受理申报后，根据申报情况组织国务院有关部门、省级网信部门、专门机构等进行安全评估。

第十一条 安全评估过程中，发现数据处理者提交的申报材料不符合要求的，国家网信部门可以要求其补充或者更正。数据处理者无正当理由不补充或者更正的，国家网信部门可以终止安全评估。

数据处理者对所提交材料的真实性负责，故意提交虚假材料的，按照评估不通过处理，并依法追究相应法律责任。

第十二条 国家网信部门应当自向数据处理者发出书面受理通知书之日起45个工作日内完成数据出境安全评估；情况复杂或者需要补充、更正材料的，可以适当延长并告知数据处理者预计延长的时间。

评估结果应当书面通知数据处理者。

第十三条 数据处理者对评估结果有异议的，可以在收到评估结果15个工作日内向国家网信部门申请复评，复评结果为最终结论。

第十四条 通过数据出境安全评估的结果有效期为2年，自评估结果出具之日起计算。在有效期内出现以下情形之一的，数据处理者应当重新申报评估：

（一）向境外提供数据的目的、方式、范围、种类和境外接收方处理数据的用途、方式发生变化影响出境数据安全的，或者延长个人信息和重要数据境外保存期限的；

（二）境外接收方所在国家或者地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形、数据处理者或者境外接收方实际控制权发生变化、数据处理者与境外接收方法律文件变更等影响出境数据安全的；

（三）出现影响出境数据安全的其他情形。

有效期届满，需要继续开展数据出境活动的，数据处理者应当在有效期届满60个工作日前重新申报评估。

第十五条 参与安全评估工作的相关机构和人员对在履行职责中知悉的国家秘密、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、非法使用。

第十六条 任何组织和个人发现数据处理者违反本办法向境外提供数据的，可以向省级以上网信部门举报。

第十七条 国家网信部门发现已经通过评估的数据出境活动在实际处理过程中不再符合数据出境安全管理要求的，应当书面通知数据处理者终止数据出境活动。数据处理者需要继续开展数据出境活动的，应当按照要求整改，整改完成后重新申报评估。

第十八条 违反本办法规定的，依据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律法规处理；构成犯罪的，依法追究刑事责任。

第十九条 本办法所称重要数据，是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据。

第二十条 本办法自2022年9月1日起施行。本办法施行前已经开展的数据出境活动，不符合本办法规定的，应当自本办法施行之日起6个月内完成整改。

02
智能汽车安全

[智能汽车创新须重视数据安全]

近段时间，小鹏、长安、比亚迪等车企纷纷下架旗下产品车外远程拍照、远程泊车等功能。这些原本智能汽车独有的酷炫功能的调整引发热议，**在智能网联时代，如何兼顾功能创新与数据隐私安全？**

智能汽车被认为是汽车发展的重要趋势，数据则是实现智能的基石。海量数据能够帮助车企有效分析驾乘人员的使用习惯，进而及时更新功能，打造出更完美的新品。但智能网联汽车已不只是交通工具，也是大型智能终端，收集数据的程度已远超公众想象。这些数据既有驾乘人员的外观特征、行为习惯等信息，更包含车辆地理位置、车外道路环境等数据，一旦泄露，轻则侵犯个人隐私，重则危及公共利益、国家安全。因此，守护好智能汽车数据，关乎用户权益，更关乎行业发展进程。

首先，完善政策法规，设置好“红绿灯”

近年来，我国数据安全立法进程明显加快，但专门针对智能汽车数据管理的政策法规仍显滞后。为此，去年以来，多部门相继出台了《汽车数据安全管理若干规定（试行）》《信息安全技术网联汽车采集数据的安全要求》等法规，搭起了智能汽车数据监管框架。但需清醒认识到，目前我国相关的政策法规仍处于初步规范阶段，监管的诸多细节仍有待明晰完善。相关部门需结合技术创新和产业发展趋势，加快完善智能网联汽车数据安全的政策法规和标准体系，为行业有序发展设置好“红绿灯”。

其次，车企要切实扛起主体责任

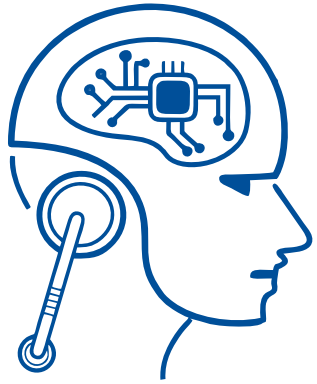
近年来，智能产品成为车企竞逐的新赛道，甚至有车企不惜以出格的功能来吸引消费者。在监管趋严的背景下，车企应提高合规意识，不再将涉及数据安全的技术当作噱头过度营销。车企还要切实履行数据安全保护义务，确保合理保存车辆状态数据，严格保护用户隐私数据。当然，合规经营只是基础，车企还应多从技术创新层面破解数据安全风险。目前已有一些车企在积极寻找技术突破口，例如智己汽车取消了人脸识别，改用采集眼球转动的信息，尽量少采集个人信息。

最后，消费者应理性看待、使用智能功能

消费者要树立“数据安全极端重要”的观念意识，并将其视为竞争性功能，进而倒逼车企重视、主动防范相关风险。消费者还应调整心理预期，不过度追逐新奇功能，更不能以泄露个人隐私甚至牺牲汽车数据安全为代价，将个人需求凌驾于公共安全之上。

守护智能汽车数据安全需要多方主体共同发力。相信随着政策法规的完善和消费者安全意识的提升，智能汽车的数据安全风险将得到有效管控，届时行业将有望驶入加速发展的“快车道”。

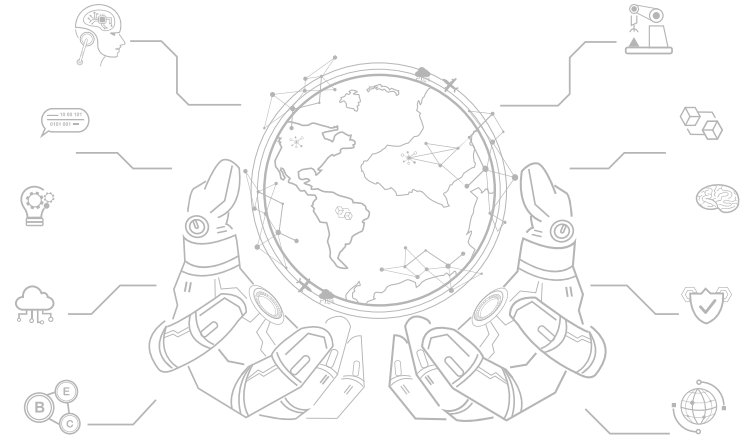
（本文来源：经济日报 作者：周 剑）



[发展人工智能不可忽视安全]

全球新一轮科技革命和产业变革方兴未艾，而作为引领新一轮科技革命和产业变革的核心驱动力量之一，人工智能近年来被广泛应用于金融、电商、医疗等领域。

风生水起之余，人工智能产业也暗藏隐忧.随着全球人工智能规模化建设和应用的加速，人工智能基础设施、设计研发及融合应用面临的安全风险正日益凸显。由中国信息通信研究院联合瑞莱智慧RealAI、百度、腾讯等单位共同撰写的《人工智能安全框架（2020年）》显示，随着深度伪造技术开源代码、APP应用增多，不法分子利用深度伪造技术制作虚假视频侵犯个人肖像权、名誉权和隐私权的现象屡见不鲜。截至2019年12月份，全网流传的深度伪造视频中，虚假色情内容占比高达96%。



而这只是问题的冰山一角。指纹和人脸识别留下的生物特征信息、自动驾驶留下的个人行踪记录、手机APP保存的个人隐私数据、医院里留存的诊断治疗记录……人工智能跑步进入人们工作生活的众多场景，用户各种行为被记录并作为数据保存起来，由此带来的数据泄露、数据伪造、算法瓶颈、隐私安全、伦理困境等问题如今正一点点浮出水面。据有关报道，今年7月份就有不法分子在电商平台贩卖人脸信息，以5角钱一份的低价打包出售后，被盗的人脸信息被用于虚假注册、电信网络诈骗等违法犯罪活动。

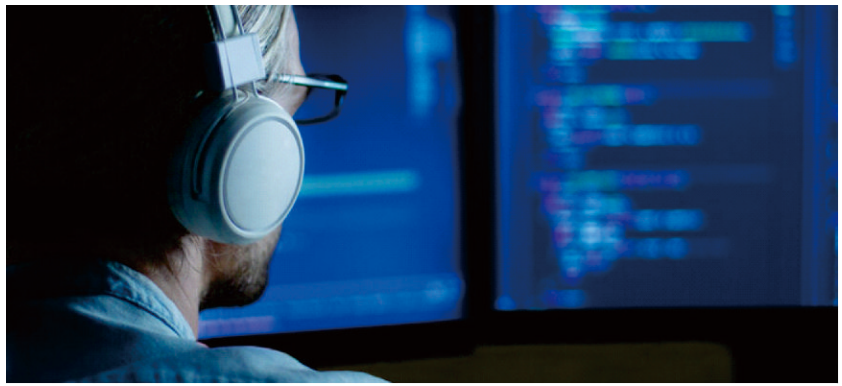
尴尬的是，《人工智能安全框架（2020年）》显示，现阶段人工智能企业主要聚焦于技术研发和产品运营，在人工智能安全方面投入相对较少、基础薄弱。目前，人工智能安全技术多处于学术研究和少量试验试用阶段，尚未形成适用于各类人工智能应用的成熟安全产品和服务体系。

人工智能产业健康有序发展，安全是重要保障，是形势所需，也是一些技术落地不可或缺的前提。离开了安全谈人工智能，犹如无水之源、无本之木。实践也已证明，时下人工智能安全需求与企业安全投入不足以及人工智能安全产品服务欠缺之间的矛盾，正成为制约人工智能产业长远发展的瓶颈。

站在发展困境与时代机遇重叠的关键时刻，业界期待产学研各界协同合作，不断完善与升级出更安全、可信、可靠的人工智能技术，扎牢人工智能安全的篱笆，让人们能安心享受这一技术红利。

04
“棱镜门”

[“棱镜门”事件十周年]



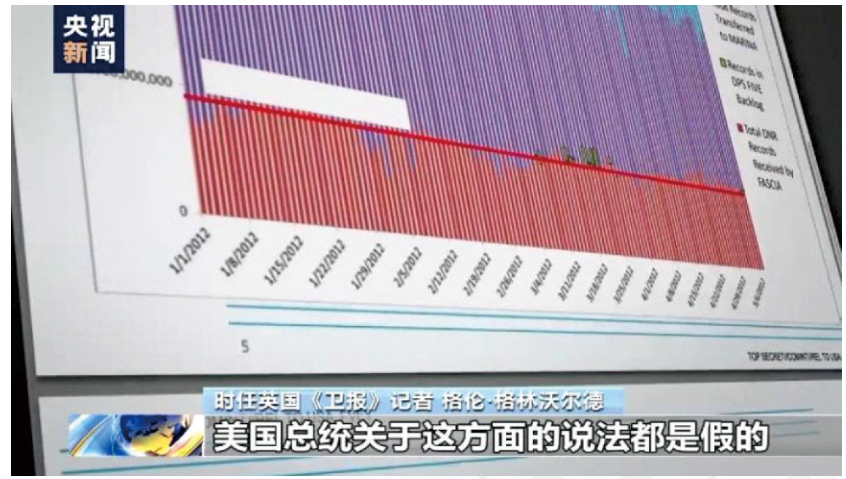
今年是美国“棱镜门”丑闻曝光十周年

2013年6月5日，英国《卫报》首次披露，美国正在开展一个代号为“棱镜”的秘密项目。美国情报机构利用微软、谷歌、苹果、脸书、雅虎等9家互联网公司及一些大型通信服务商提供的数据，肆意追踪民众的私人关系与社会活动，对美国国内外进行大规模监听。这一消息引发美国国内国外的广泛抗议。

美情报机构通过“棱镜”计划监听全球

2013年6月，美国前中央情报局雇员斯诺登向英国《卫报》、美国《华盛顿邮报》等媒体揭露了“棱镜”计划的真相。“棱镜”计划的正式名称为“us-984xn”，是由美国国家安全局和联邦调查局于2007年启动的秘密监听项目。美国情报机构通过接入网络公司的中心服务器，直接接触用户数据，实时跟踪用户电子邮件、聊天记录、视频、音频、文件、照片等上网信息，全面监控特定目标及其联系人的一举一动。“棱镜”计划的监听范围不仅覆盖美国国内，还包括多国政要和民众，德国、法国等美国盟友也不例外。

“棱镜”的监听范围之广、程度之深让人咋舌，遭到多方批评。对此时任美国总统奥巴马在记者会上回应称，美国情报机构只是收集数据，并没有“听电话、看短信、查电子邮件内容”，并声称此举是为了美国反恐和国家安全的需要。曝光棱镜门的时任英国《卫报》记者对这一说法嗤之以鼻。



时任英国《卫报》记者 格伦·格林沃尔德：“奥巴马说，美国国家安全局没有监听美国人的电话和查看他们的电子邮件，这一说法绝对是错误的”。我们有文件证明，美国总统关于这方面的说法都是假的。这份文件揭露的是美国国家安全局的监听系统并非针对非常坏的人或恐怖分子，而是不分青红皂白地、批量地针对美国公民和世界各地的其他公民。

“棱镜门”曝光后引发美国国内外广泛抗议

“棱镜门”丑闻令美国的欧洲盟友大为震惊。时任欧盟外交与安全政策高级代表阿什顿要求美方就监听事件立即进行澄清。时任法国总统奥朗德要求美国立即停止监听行为。德国媒体披露，时任德国总理默克尔当时已被美国情报机构监听长达十几年，引发德国强烈不满。

时任德国总理 默克尔：针对美国国家安全局的行为，我一再向美国政府明确表示，监听盟友是不可接受的。

棱镜计划将美国民众的个人隐私毫无遮蔽地暴露在政府面前，这也引发了美国国内的大面积抗议，华盛顿、纽约、费城、波士顿、芝加哥及旧金山等城市都有民众举行示威，反对这种无差别监听行为。美国最具影响力的民权组织——美国公民自由联盟正式起诉联邦政府，指控其“棱镜”计划侵犯言论自由和公民隐私权、违反宪法，并请求法院下令中止这一项目。

当地时间7日，中央广播电视总台记者采访到了法国通信技术专家勒费比尔。勒费比尔认为，“棱镜门”事件虽然已经过去十年，但是美国当局对其他国家的监听不但没有收敛，反而变本加厉。只要是美方能够涉及的领域，无论合理与否，监听行动都一直在进行。

俄罗斯国际事务理事会主任科尔图诺夫在接受总台记者采访时表示，美国出于所谓的“维护国家安全”目的，大搞国际非法监听活动，美式霸权祸害世界。

俄罗斯国际事务理事会主任　科尔图诺夫：美国异常担心自己的内政被其他国家干涉，但与此同时，美国却不止一次利用监听手段对其他国家的内部政治进程施加影响。美国的监听行为会对国际合作造成损害，我还认为这有损于美国的长期经济和政治利益。

最先披露“棱镜门”丑闻的英国《卫报》7日刊文称，10年后看来，“棱镜门”丑闻的曝光，虽然迫使美国政府解密了部分情报部门运作的细节，但是类似变化并没有触及问题的核心。

文章援引曝光“棱镜门”的前英国《卫报》记者格伦·格林沃尔德的话说，美国政府至今仍在继续其监听行径，其方式甚至比10年前所披露出来的更糟糕、更极端。针对美国在监听问题上的种种作为，格林沃尔德说，美国最擅长的事情之一，就是总要打造出一个新的敌人来令美国人民恐惧，总要编造出理由来让美国人民相信，美国政府有必要秘密运作、大搞间谍活动、同时拥有无限的权力。

“棱镜门”事件曝光十周年
中国外交部：美国是网络空间和平与稳定的“破坏者”

中国外交部：美国是网络空间和平与稳定的“破坏者”。今年是“棱镜门”事件曝光十周年。十年前，美国前防务承包商雇员斯诺登向多家媒体爆料，用大量证据揭露美国政府长期以所谓“反恐”为名监听监视世界各国的行径，引发国际社会强烈谴责。中国外交部发言人汪文斌在6月9日的记者会上表示，“棱镜门”揭开了美国这个“黑客帝国”的真面目。十年过去了，“黑客帝国”不仅没有放慢自己的脚步，反而更加肆无忌惮，试图将世更多置于自己的网络窃密阴影之下。

网络安全知识笔记