师德师风教育学习资料

2023 年第 10 期(总第 20 期)

党委教师工作部编　　2023 年 12 月 28 日

反诈防骗专题

反诈防骗学习资料

一、图文学习资料

1.防范电信网络诈骗宣传手册 2023 版(国家反诈中心)

https://rsc.jxnu.edu.cn/2023/1228/c10381a255878/page.htm

2.防范电信网络诈骗应知应会知识手册(江西师范大学保卫处整理汇编)

https://rsc.jxnu.edu.cn/2023/1228/c10381a255879/page.htm

二、视频学习资料

1.秒懂“反电诈法” 请看这个动画视频

https://baijiahao.baidu.com/s?id=1751747198616263944

2.反电信网络诈骗——宣传片

https://www.ixigua.com/6857887967466226183?wid_try=1

3.反电信网络诈骗指南

https://weibo.com/tv/show/1034:4757359483093025

4.央视《焦点访谈》：“五大利器”防电诈

https://haokan.baidu.com/v?pd=wisenatural&vid=9024837541248464 84

5.反电信网络诈骗手绘

https://v.qq.com/x/page/d0539doo3cw.html

6.反诈 电信网络诈骗花样多，提高警惕，谨防诈骗！ (国家反诈中心)

https://haokan.baidu.com/v?pd=wisenatural&vid=3904133113648447214

7.全民反电诈 诈骗无孔不入，反电信网络诈骗，国家正在行动！

https://haokan.baidu.com/v?pd=wisenatural&vid=9861556967483246139

8.反电信网络诈骗法普法宣传：律师教你几招，有效防范电信网络诈骗！

https://v.qq.com/x/page/k3534u59dk4.html

9.电信网络诈骗五种常见套路

https://weibo.com/tv/show/1034:4877417240789043

10.什么是电信网络诈骗？都有哪些套路呢？听完这个快板你就了解了

https://haokan.baidu.com/v?pd=wisenatural&vid=4662118178304266126

(来源：江西师范大学党委教师工作部整理汇编而成)

诈骗行为所涉的法律规定(节选)

一、中华人民共和国刑法(2020 修正)

第一百九十二条 以非法占有为目的，使用诈骗方法非法集资，数额较大的，处三年以上七年以下有期徒刑，并处罚金；数额巨大或者有其他严重情节的，处七年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。

单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照前款的规定处罚。

第一百九十三条 有下列情形之一，以非法占有为目的，诈骗银行或者其他金融机构的贷款，数额较大的，处五年以下有期徒刑或者拘役，并处二万元以上二十万元以下罚金；数额巨大或者有其他严重情节的，处五年以上十年以下有期徒刑，并处五万元以上五十万元以下罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处五万元以上五十万元以下罚金或者没收财产：

(一)编造引进资金、项目等虚假理由的；

(二)使用虚假的经济合同的；

(三)使用虚假的证明文件的；

(四)使用虚假的产权证明作担保或者超出抵押物价值重复担保的；

(五)以其他方法诈骗贷款的。

第一百九十四条 有下列情形之一，进行金融票据诈骗活动，数额较大的，处五年以下有期徒刑或者拘役，并处二万元以上二十万元以下罚金；数额巨大或者有其他严重情节的，处五年以上十年以下有期徒刑，并处五万元以上五十万元以下罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处五万元以上五十万元以下罚金或者没收财产：

(一)明知是伪造、变造的汇票、本票、支票而使用的；

(二)明知是作废的汇票、本票、支票而使用的；

(三)冒用他人的汇票、本票、支票的；

(四)签发空头支票或者与其预留印鉴不符的支票，骗取财物的；

(五)汇票、本票的出票人签发无资金保证的汇票、本票或者在出票时作虚假记载，骗取财物的。

使用伪造、变造的委托收款凭证、汇款凭证、银行存单等其他银行结算凭证的，依照前款的规定处罚。

第一百九十五条 有下列情形之一，进行信用证诈骗活动的，处五年以下有期徒刑或者拘役，并处二万元以上二十万元以下罚金；数额巨大或者有其他严重情节的，处五年以上十年以下有期徒刑，并处五万元以上五十万元以下罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处五万元以上五十万元以下罚金或者没收财产：

(一)使用伪造、变造的信用证或者附随的单据、文件的；

(二)使用作废的信用证的；

(三)骗取信用证的；

(四)以其他方法进行信用证诈骗活动的。

第一百九十六条 有下列情形之一，进行信用卡诈骗活动，数额较大的，处五年以下有期徒刑或者拘役，并处二万元以上二十万元以下罚金；数额巨大或者有其他严重情节的，处五年以上十年以下有期徒刑，并处五万元以上五十万元以下罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处五万元以上五十万元以下罚金或者没收财产：

(一)使用伪造的信用卡，或者使用以虚假的身份证明骗领的信用卡的；

(二)使用作废的信用卡的；

(三)冒用他人信用卡的；

(四)恶意透支的。

前款所称恶意透支，是指持卡人以非法占有为目的，超过规定限额或者规定期限透支，并且经发卡银行催收后仍不归还的行为。

盗窃信用卡并使用的，依照本法第二百六十四条的规定定罪处罚。

第一百九十七条 使用伪造、变造的国库券或者国家发行的其他有价证券，进行诈骗活动，数额较大的，处五年以下有期徒刑或者拘役，并处二万元以上二十万元以下罚金；数额巨大或者有其他严重情节的，处五年以上十年以

下有期徒刑，并处五万元以上五十万元以下罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处五万元以上五十万元以下罚金或者没收财产。

第一百九十八条 有下列情形之一，进行保险诈骗活动，数额较大的，处五年以下有期徒刑或者拘役，并处一万元以上十万元以下罚金；数额巨大或者有其他严重情节的，处五年以上十年以下有期徒刑，并处二万元以上二十万元以下罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑，并处二万元以上二十万元以下罚金或者没收财产：

(一)投保人故意虚构保险标的，骗取保险金的；

(二)投保人、被保险人或者受益人对发生的保险事故编造虚假的原因或者夸大损失的程度，骗取保险金的；

(三)投保人、被保险人或者受益人编造未曾发生的保险事故，骗取保险金的；

(四)投保人、被保险人故意造成财产损失的保险事故，骗取保险金的；

(五)投保人、受益人故意造成被保险人死亡、伤残或者疾病，骗取保险金的。

有前款第四项、第五项所列行为，同时构成其他犯罪的，依照数罪并罚的规定处罚。

单位犯第一款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，处五年以下有期徒刑或者拘役；数额巨大或者有其他严重情节的，处五年以上十年以下有期徒刑；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑。

保险事故的鉴定人、证明人、财产评估人故意提供虚假的证明文件，为他人诈骗提供条件的，以保险诈骗的共犯论处。

第二百条 单位犯本节第一百九十四条、第一百九十五条规定之罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，处五年以下有期徒刑或者拘役，可以并处罚金；数额巨大或者有其他严重情节的，处五年以上十年以下有期徒刑，并处罚金；数额特别巨大或者有其他特别严重情节

的，处十年以上有期徒刑或者无期徒刑，并处罚金。

第二百六十六条 诈骗公私财物，数额较大的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；数额巨大或者有其他严重情节的，处三年以上十年以下有期徒刑，并处罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。本法另有规定的，依照规定。

二、最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见(法发〔2016〕32号)

二、依法严惩电信网络诈骗犯罪

(一)根据《最高人民法院、最高人民检察院关于办理诈骗刑事案件具体应用法律若干问题的解释》第一条的规定，利用电信网络技术手段实施诈骗，诈骗公私财物价值三千元以上、三万元以上、五十万元以上的，应当分别认定为刑法第二百六十六条规定的“数额较大”“数额巨大”“数额特别巨大”。

二年内多次实施电信网络诈骗未经处理，诈骗数额累计计算构成犯罪的，应当依法定罪处罚。

(二)实施电信网络诈骗犯罪，达到相应数额标准，具有下列情形之一的，酌情从重处罚：

1.造成被害人或其近亲属自杀、死亡或者精神失常等严重后果的；

2.冒充司法机关等国家机关工作人员实施诈骗的；

3.组织、指挥电信网络诈骗犯罪团伙的；

4.在境外实施电信网络诈骗的；

5.曾因电信网络诈骗犯罪受过刑事处罚或者二年内曾因电信网络诈骗受过行政处罚的；

6.诈骗残疾人、老年人、未成年人、在校学生、丧失劳动能力人的财物，或者诈骗重病患者及其亲属财物的；

7.诈骗救灾、抢险、防汛、优抚、扶贫、移民、救济、医疗等款物的；

8.以赈灾、募捐等社会公益、慈善名义实施诈骗的；

9.利用电话追呼系统等技术手段严重干扰公安机关等部门工作的；

10.利用“钓鱼网站”链接、“木马”程序链接、网络渗透等隐蔽技术手段实施诈骗的。

(三)实施电信网络诈骗犯罪，诈骗数额接近“数额巨大”“数额特别巨大”的标准，具有前述第(二)条规定的情形之一的，应当分别认定为刑法第二百六十六条规定的“其他严重情节”“其他特别严重情节”。

上述规定的“接近”，一般应掌握在相应数额标准的百分之八十以上。

(四)实施电信网络诈骗犯罪，犯罪嫌疑人、被告人实际骗得财物的，以诈骗罪(既遂)定罪处罚。诈骗数额难以查证，但具有下列情形之一的，应当认定为刑法第二百六十六条规定的“其他严重情节”，以诈骗罪(未遂)定罪处罚：

1.发送诈骗信息五千条以上的，或者拨打诈骗电话五百人次以上的；

2.在互联网上发布诈骗信息，页面浏览量累计五千次以上的。

具有上述情形，数量达到相应标准十倍以上的，应当认定为刑法第二百六十六条规定的“其他特别严重情节”，以诈骗罪(未遂)定罪处罚。

上述“拨打诈骗电话”，包括拨出诈骗电话和接听被害人回拨电话。反复拨打、接听同一电话号码，以及反复向同一被害人发送诈骗信息的，拨打、接听电话次数、发送信息条数累计计算。

因犯罪嫌疑人、被告人故意隐匿、毁灭证据等原因，致拨打电话次数、发送信息条数的证据难以收集的，可以根据经查证属实的日拨打人次数、日发送信息条数，结合犯罪嫌疑人、被告人实施犯罪的时间、犯罪嫌疑人、被告人的供述等相关证据，综合予以认定。

(五)电信网络诈骗既有既遂，又有未遂，分别达到不同量刑幅度的，依照处罚较重的规定处罚；达到同一量刑幅度的，以诈骗罪既遂处罚。

(六)对实施电信网络诈骗犯罪的被告人裁量刑罚，在确定量刑起点、基准刑时，一般应就高选择。确定宣告刑时，应当综合全案事实情节，准确把握从重、从轻量刑情节的调节幅度，保证罪责刑相适应。

(七)对实施电信网络诈骗犯罪的被告人，应当严格控制适用缓刑的范围，严格掌握适用缓刑的条件。

(八)对实施电信网络诈骗犯罪的被告人，应当更加注重依法适用财产刑，加大经济上的惩罚力度，最大限度剥夺被告人再犯的能力。

三、中华人民共和国反电信网络诈骗法

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。

(来源：江西师范大学党委教师工作部整理汇编而成)

中华人民共和国反电信网络诈骗法

中华人民共和国主席令

第一一九号

《中华人民共和国反电信网络诈骗法》已由中华人民共和国第十三届全国人民代表大会常务委员会第三十六次会议于2022年9月2日通过，现予公布，自2022年12月1日起施行。

中华人民共和国主席　习近平

2022年9月2日

中华人民共和国反电信网络诈骗法

(2022 年 9 月 2 日第十三届全国人民代表大会常务委员会第三十六次会议通过)

目　　录

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。

(来源：中国人大网 2022-09-02)

中华人民共和国网络安全法

中华人民共和国主席令

(第五十三号)

《中华人民共和国网络安全法》已由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于2016年11月7日通过，现予公布，自2017年6月1日起施行。

中华人民共和国主席 习近平

2016年11月7日

中华人民共和国网络安全法

(2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过)

目录

第一章　总 则

第一条　为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

第二条　在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

第三条　国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

第四条　国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

第五条　国家采取措施，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，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

第六条　国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

第七条　国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

第八条　国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关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网络安全保护和监督管理工作。

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

第九条 网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

第十条 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

第十一条 网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

第十二条 国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

第十三条 国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

第十四条 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

第二章　网络安全支持与促进

第十五条　国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

第十六条　国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

第十七条　国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

第十八条　国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

国家支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。

第十九条　各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。

大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

第二十条　国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

第三章　网络运行安全

第一节　一般规定

第二十一条　国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

(一)制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

(二)采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

(三)采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

(四)采取数据分类、重要数据备份和加密等措施；

(五)法律、行政法规规定的其他义务。

第二十二条　网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

第二十三条　网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

第二十四条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

第二十五条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第二十六条 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

第二十七条 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

第二十八条 网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

第二十九条 国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。

有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

第三十条 网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

第二节 关键信息基础设施的运行安全

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，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、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

第三十二条 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

第三十三条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第三十四条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：

(一)设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

(二)定期对从业人员进行网络安全教育、技术培训和技能考核；

(三)对重要系统和数据库进行容灾备份；

(四)制定网络安全事件应急预案，并定期进行演练；

(五)法律、行政法规规定的其他义务。

第三十五条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

第三十六条 关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

第三十七条 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个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

第三十九条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

(一)对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；

(二)定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；

(三)促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；

(四)对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

第四章 网络信息安全

第四十条 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

第四十一条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

第四十二条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第四十三条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

第四十四条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第四十五条 依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

第四十六条 任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

第四十七条 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

第四十八条 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

第四十九条 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

第五十条 国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

第五章 监测预警与应急处置

第五十一条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

第五十二条 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

第五十三条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第五十四条 网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：

(一)要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测；

(二)组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；

(三)向社会发布网络安全风险预警，发布避免、减轻危害的措施。

第五十五条 发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

第五十六条 省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

第五十七条 因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

第五十八条 因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

第六章 法律责任

第五十九条 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改

正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

第六十条 违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：

(一)设置恶意程序的；

(二)对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；

(三)擅自终止为其产品、服务提供安全维护的。

第六十一条 网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，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、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。

第六十二条 违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，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、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五千元以上五万元以下罚款。

第六十三条 违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，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。

违反本法第二十七条规定，受到治安管理处罚的人员，五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。

第六十四条 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

第六十五条 关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，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。

第六十六条 关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、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。

第六十七条 违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。

单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，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。

第六十八条 网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、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。

电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。

第六十九条 网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，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：

(一)不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的；

(二)拒绝、阻碍有关部门依法实施的监督检查的；

(三)拒不向公安机关、国家安全机关提供技术支持和协助的。

第七十条 发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。

第七十一条 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。

第七十二条 国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；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。

第七十三条 网信部门和有关部门违反本法第三十条规定，将在履行网络安全保护职责中获取的信息用于其他用途的，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。

网信部门和有关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。

第七十四条 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。

第七十五条 境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

第七章 附 则

第七十六条 本法下列用语的含义：

(一)网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

(二)网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

(三)网络运营者，是指网络的所有者、管理者和网络服务提供者。

(四)网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

(五)个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

第七十七条 存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。

第七十八条 军事网络的安全保护，由中央军事委员会另行规定。

第七十九条 本法自 2017 年 6 月 1 日起施行。

(来源：中国人大网 2016-11-07)

中华人民共和国个人信息保护法

(2021 年 8 月 20 日第十三届全国人民代表大会常务委员会第三十次会议通过)

目　　录

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。

第八章　附　　则

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。

(来源：中国人大网 2021-08-20)

中华人民共和国反洗钱法

(2006 年 10 月 31 日第十届全国人民代表大会常务委员会第二十四次会议通过)

目录

第一章　总则

第一条　为了预防洗钱活动，维护金融秩序，遏制洗钱犯罪及相关犯罪，制定本法。

第二条　本法所称反洗钱，是指为了预防通过各种方式掩饰、隐瞒毒品犯罪、黑社会性质的组织犯罪、恐怖活动犯罪、走私犯罪、贪污贿赂犯罪、破坏金融管理秩序犯罪、金融诈骗犯罪等犯罪所得及其收益的来源和性质的洗钱活动，依照本法规定采取相关措施的行为。

第三条　在中华人民共和国境内设立的金融机构和按照规定应当履行反洗钱义务的特定非金融机构，应当依法采取预防、监控措施，建立健全客户身份识别制度、客户身份资料和交易记录保存制度、大额交易和可疑交易报告制度，履行反洗钱义务。

第四条　国务院反洗钱行政主管部门负责全国的反洗钱监督管理工作。国务院有关部门、机构在各自的职责范围内履行反洗钱监督管理职责。

国务院反洗钱行政主管部门、国务院有关部门、机构和司法机关在反洗钱工作中应当相互配合。

第五条　对依法履行反洗钱职责或者义务获得的客户身份资料和交易信息，应当予以保密；非依法律规定，不得向任何单位和个人提供。

反洗钱行政主管部门和其他依法负有反洗钱监督管理职责的部门、机构履行反洗钱职责获得的客户身份资料和交易信息，只能用于反洗钱行政调查。

司法机关依照本法获得的客户身份资料和交易信息，只能用于反洗钱刑事诉讼。

第六条　履行反洗钱义务的机构及其工作人员依法提交大额交易和可疑交易报告，受法律保护。

第七条　任何单位和个人发现洗钱活动，有权向反洗钱行政主管部门或者公安机关举报。接受举报的机关应当对举报人和举报内容保密。

第二章　反洗钱监督管理

第八条　国务院反洗钱行政主管部门组织、协调全国的反洗钱工作，负责反洗钱的资金监测，制定或者会同国务院有关金融监督管理机构制定金融机构反洗钱规章，监督、检查金融机构履行反洗钱义务的情况，在职责范围内调查可疑交易活动，履行法律和国务院规定的有关反洗钱的其他职责。

国务院反洗钱行政主管部门的派出机构在国务院反洗钱行政主管部门的授权范围内，对金融机构履行反洗钱义务的情况进行监督、检查。

第九条　国务院有关金融监督管理机构参与制定所监督管理的金融机构反洗钱规章，对所监督管理的金融机构提出按照规定建立健全反洗钱内部控制制度的要求，履行法律和国务院规定的有关反洗钱的其他职责。

第十条　国务院反洗钱行政主管部门设立反洗钱信息中心，负责大额交易和可疑交易报告的接收、分析，并按照规定向国务院反洗钱行政主管部门报告分析结果，履行国务院反洗钱行政主管部门规定的其他职责。

第十一条　国务院反洗钱行政主管部门为履行反洗钱资金监测职责，可以从国务院有关部门、机构获取所必需的信息，国务院有关部门、机构应当提供。

国务院反洗钱行政主管部门应当向国务院有关部门、机构定期通报反洗钱

工作情况。

第十二条　海关发现个人出入境携带的现金、无记名有价证券超过规定金额的，应当及时向反洗钱行政主管部门通报。

前款应当通报的金额标准由国务院反洗钱行政主管部门会同海关总署规定。

第十三条　反洗钱行政主管部门和其他依法负有反洗钱监督管理职责的部门、机构发现涉嫌洗钱犯罪的交易活动，应当及时向侦查机关报告。

第十四条　国务院有关金融监督管理机构审批新设金融机构或者金融机构增设分支机构时，应当审查新机构反洗钱内部控制制度的方案；对于不符合本法规定的设立申请，不予批准。

第三章　金融机构反洗钱义务

第十五条　金融机构应当依照本法规定建立健全反洗钱内部控制制度，金融机构的负责人应当对反洗钱内部控制制度的有效实施负责。

金融机构应当设立反洗钱专门机构或者指定内设机构负责反洗钱工作。

第十六条　金融机构应当按照规定建立客户身份识别制度。

金融机构在与客户建立业务关系或者为客户提供规定金额以上的现金汇款、现钞兑换、票据兑付等一次性金融服务时，应当要求客户出示真实有效的身份证件或者其他身份证明文件，进行核对并登记。

客户由他人代理办理业务的，金融机构应当同时对代理人和被代理人的身份证件或者其他身份证明文件进行核对并登记。

与客户建立人身保险、信托等业务关系，合同的受益人不是客户本人的，金融机构还应当对受益人的身份证件或者其他身份证明文件进行核对并登记。

金融机构不得为身份不明的客户提供服务或者与其进行交易，不得为客户开立匿名账户或者假名账户。

金融机构对先前获得的客户身份资料的真实性、有效性或者完整性有疑问的，应当重新识别客户身份。

任何单位和个人在与金融机构建立业务关系或者要求金融机构为其提供一

次性金融服务时，都应当提供真实有效的身份证件或者其他身份证明文件。

第十七条　金融机构通过第三方识别客户身份的，应当确保第三方已经采取符合本法要求的客户身份识别措施；第三方未采取符合本法要求的客户身份识别措施的，由该金融机构承担未履行客户身份识别义务的责任。

第十八条　金融机构进行客户身份识别，认为必要时，可以向公安、工商行政管理等部门核实客户的有关身份信息。

第十九条　金融机构应当按照规定建立客户身份资料和交易记录保存制度。

在业务关系存续期间，客户身份资料发生变更的，应当及时更新客户身份资料。

客户身份资料在业务关系结束后、客户交易信息在交易结束后，应当至少保存五年。

金融机构破产和解散时，应当将客户身份资料和客户交易信息移交国务院有关部门指定的机构。

第二十条　金融机构应当按照规定执行大额交易和可疑交易报告制度。

金融机构办理的单笔交易或者在规定期限内的累计交易超过规定金额或者发现可疑交易的，应当及时向反洗钱信息中心报告。

第二十一条　金融机构建立客户身份识别制度、客户身份资料和交易记录保存制度的具体办法，由国务院反洗钱行政主管部门会同国务院有关金融监督管理机构制定。金融机构大额交易和可疑交易报告的具体办法，由国务院反洗钱行政主管部门制定。

第二十二条　金融机构应当按照反洗钱预防、监控制度的要求，开展反洗钱培训和宣传工作。

第四章　反洗钱调查

第二十三条　国务院反洗钱行政主管部门或者其省一级派出机构发现可疑交易活动，需要调查核实的，可以向金融机构进行调查，金融机构应当予以配合，如实提供有关文件和资料。

调查可疑交易活动时，调查人员不得少于二人，并出示合法证件和国务院反洗钱行政主管部门或者其省一级派出机构出具的调查通知书。调查人员少于二人或者未出示合法证件和调查通知书的，金融机构有权拒绝调查。

第二十四条　调查可疑交易活动，可以询问金融机构有关人员，要求其说明情况。

询问应当制作询问笔录。询问笔录应当交被询问人核对。记载有遗漏或者差错的，被询问人可以要求补充或者更正。被询问人确认笔录无误后，应当签名或者盖章；调查人员也应当在笔录上签名。

第二十五条　调查中需要进一步核查的，经国务院反洗钱行政主管部门或者其省一级派出机构的负责人批准，可以查阅、复制被调查对象的账户信息、交易记录和其他有关资料；对可能被转移、隐藏、篡改或者毁损的文件、资料，可以予以封存。

调查人员封存文件、资料，应当会同在场的金融机构工作人员查点清楚，当场开列清单一式二份，由调查人员和在场的金融机构工作人员签名或者盖章，一份交金融机构，一份附卷备查。

第二十六条　经调查仍不能排除洗钱嫌疑的，应当立即向有管辖权的侦查机关报案。客户要求将调查所涉及的账户资金转往境外的，经国务院反洗钱行政主管部门负责人批准，可以采取临时冻结措施。

侦查机关接到报案后，对已依照前款规定临时冻结的资金，应当及时决定是否继续冻结。侦查机关认为需要继续冻结的，依照刑事诉讼法的规定采取冻结措施；认为不需要继续冻结的，应当立即通知国务院反洗钱行政主管部门，国务院反洗钱行政主管部门应当立即通知金融机构解除冻结。

临时冻结不得超过四十八小时。金融机构在按照国务院反洗钱行政主管部门的要求采取临时冻结措施后四十八小时内，未接到侦查机关继续冻结通知的，应当立即解除冻结。

第五章　反洗钱国际合作

第二十七条　中华人民共和国根据缔结或者参加的国际条约，或者按照平

等互惠原则，开展反洗钱国际合作。

第二十八条　国务院反洗钱行政主管部门根据国务院授权，代表中国政府与外国政府和有关国际组织开展反洗钱合作，依法与境外反洗钱机构交换与反洗钱有关的信息和资料。

第二十九条　涉及追究洗钱犯罪的司法协助，由司法机关依照有关法律的规定办理。

第六章　法律责任

第三十条　反洗钱行政主管部门和其他依法负有反洗钱监督管理职责的部门、机构从事反洗钱工作的人员有下列行为之一的，依法给予行政处分：

(一)违反规定进行检查、调查或者采取临时冻结措施的；

(二)泄露因反洗钱知悉的国家秘密、商业秘密或者个人隐私的；

(三)违反规定对有关机构和人员实施行政处罚的；

(四)其他不依法履行职责的行为。

第三十一条　金融机构有下列行为之一的，由国务院反洗钱行政主管部门或者其授权的设区的市一级以上派出机构责令限期改正；情节严重的，建议有关金融监督管理机构依法责令金融机构对直接负责的董事、高级管理人员和其他直接责任人员给予纪律处分：

(一)未按照规定建立反洗钱内部控制制度的；

(二)未按照规定设立反洗钱专门机构或者指定内设机构负责反洗钱工作的；

(三)未按照规定对职工进行反洗钱培训的。

第三十二条　金融机构有下列行为之一的，由国务院反洗钱行政主管部门或者其授权的设区的市一级以上派出机构责令限期改正；情节严重的，处二十万元以上五十万元以下罚款，并对直接负责的董事、高级管理人员和其他直接责任人员，处一万元以上五万元以下罚款：

(一)未按照规定履行客户身份识别义务的；

(二)未按照规定保存客户身份资料和交易记录的；

(三)未按照规定报送大额交易报告或者可疑交易报告的；

(四)与身份不明的客户进行交易或者为客户开立匿名账户、假名账户的；

(五)违反保密规定，泄露有关信息的；

(六)拒绝、阻碍反洗钱检查、调查的；

(七)拒绝提供调查材料或者故意提供虚假材料的。

金融机构有前款行为，致使洗钱后果发生的，处五十万元以上五百万元以下罚款，并对直接负责的董事、高级管理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；情节特别严重的，反洗钱行政主管部门可以建议有关金融监督管理机构责令停业整顿或者吊销其经营许可证。

对有前两款规定情形的金融机构直接负责的董事、高级管理人员和其他直接责任人员，反洗钱行政主管部门可以建议有关金融监督管理机构依法责令金融机构给予纪律处分，或者建议依法取消其任职资格、禁止其从事有关金融行业工作。

第三十三条　违反本法规定，构成犯罪的，依法追究刑事责任。

第七章　附则

第三十四条　本法所称金融机构，是指依法设立的从事金融业务的政策性银行、商业银行、信用合作社、邮政储汇机构、信托投资公司、证券公司、期货经纪公司、保险公司以及国务院反洗钱行政主管部门确定并公布的从事金融业务的其他机构。

第三十五条　应当履行反洗钱义务的特定非金融机构的范围、其履行反洗钱义务和对其监督管理的具体办法，由国务院反洗钱行政主管部门会同国务院有关部门制定。

第三十六条　对涉嫌恐怖活动资金的监控适用本法；其他法律另有规定的，适用其规定。

第三十七条　本法自 2007 年 1 月 1 日起施行。

(来源：中国人大网 2006-10-31)