网络犯罪防治法

（征求意见稿）

第一章　总 则

第一条 为了预防、遏制和治理网络犯罪活动，维护国家安全、社会稳定和网络秩序，保护公民和组织的合法权益，根据宪法，制定本法。

第二条 在中华人民共和国境内开展网络犯罪防治及其监督管理，适用本法。

在境外的中华人民共和国公民以及向中华人民共和国境内用户提供服务的境外组织、个人实施违反本法规定的行为，损害中华人民共和国国家安全、公共利益或者公民和组织合法权益的，依法追究法律责任。

第三条 网络犯罪防治工作应当坚持中国共产党的领导，贯彻总体国家安全观，统筹发展与安全，按照打防结合、防范为先、源头治理、协同联动的原则，推进线上线下一体化防治，建立网络犯罪综合防治体系。

网络犯罪防治工作应当保障网络服务正常运营，维护电信、金融、互联网等服务提供者合法权益，营造健康有序的网络环境。

第四条 国务院公安部门牵头负责网络犯罪防治工作。国家网

信部门、新闻出版部门，国务院电信、金融、市场监管和外交、教育、商务、文化和旅游、广播电视等有关主管部门，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网络犯罪防治工作。有关主管部门应当与国务院公安部门密切配合，共同做好网络犯罪防治工作。

县级以上人民政府统筹、协调、督促和指导有关部门在各自职责范围内做好网络犯罪防治工作。县级以上人民政府有关部门的网络犯罪防治监督管理职责，按照国家有关规定确定。

第五条 电信、金融、互联网等服务提供者应当依照本法及有关法律、行政法规的规定和国家标准的强制性要求，建立落实网络安全、信息安全、数据安全管理制度，采取技术措施和其他必要措施，依法履行与其服务类型、经营规模、能力相符的网络犯罪防治义务。

第六条 任何个人和组织有权向公安机关等部门举报涉及网络犯罪的线索。

有关部门应当及时依法处理相关线索，保护举报人合法权益。对举报网络犯罪或者在网络犯罪防治工作中做出突出贡献的单位和个人，按照国家有关规定给予表彰、奖励。

电信、金融、互联网等服务提供者应当设置便捷的渠道，接受个人、组织有关网络犯罪的投诉、举报，并及时依法依规处理。

第七条 公安机关依托国家网络与信息安全信息通报机制，加强网络犯罪防治信息收集、分析和通报工作，按照规定统一发布网

络犯罪防治监测预警信息。

公安机关应当促进有关部门之间网络犯罪信息共享，加强与电信、金融、互联网等服务提供者网络犯罪形势等信息共享。

第八条 国家鼓励、扶持人工智能等网络犯罪防治技术的研究开发和推广应用，强化对人工智能等新技术新应用的安全管理。

第九条 国家鼓励和支持网络相关行业组织开展网络新技术新应用监测分析、网络犯罪态势及产业链条分析、网络犯罪风险动态评估，制定网络犯罪防治行为规范，加强网络犯罪防治行业自律、信用惩戒等工作。

第十条 各级人民政府及其有关部门应当组织开展经常性的网络犯罪防治宣传教育，指导、督促有关单位做好网络犯罪防治宣传教育工作。

学校等教育机构应当将网络犯罪防治纳入教育教学内容，广播、电视、报刊等媒体和互联网平台应当积极开展网络犯罪防治宣传，普及网络犯罪防治知识。

电信、金融、互联网等服务提供者应当采取针对性的网络犯罪防治宣传，针对异常网络行为对相关用户推送网络犯罪提示信息。

第二章 网络基础资源管理

第十一条 任何个人和组织开立移动电话卡、物联网卡、银行账户、支付账户，应当提供真实身份信息，不得实施下列行为

扰乱实名制管理:

（一）使用伪造、变造的身份证件、虚假身份信息等开立移动电话卡、物联网卡、银行账户、支付账户的;

（二）收购、租用、出售、出租银行账户、支付账户，或者未办理过户手续收购、租用、出售、出租移动电话卡、物联网卡，或者明知被用于违法犯罪而出借移动电话卡、物联网卡、银行账户、支付账户的;

（三）非法买卖境外移动电话卡、物联网卡、银行账户、支付账户的;

（四）违反国家有关规定，将物联网卡用于注册网络账号等非指定用途的;

（五）其他扰乱电信、金融实名制管理的行为。

第十二条 任何个人和组织办理互联网信息发布、即时通讯等服务，应当提供真实身份信息，不得实施下列行为扰乱网络实名制管理:

（一）使用虚假身份信息、营业执照，冒用他人身份信息、营业执照、电话号码、邮箱，或者使用物联网卡等办理互联网服务的;

（二）违法违规收购、租用、出售、出租网络账号，或者明知被用于违法犯罪而出借网络账号的;

（三）使用网络地址切换工具、批量电话卡控制工具等规避网络运营者账号注册审核规则及其他措施，大量注册网络账号的;

（四）为已被依法依规采取封禁等措施的网络账号提供解封等技术支持或者帮助的;

（五）无正当理由大量持有非本人注册的网络账号的;

（六）其他扰乱网络实名制管理的行为。

第十三条 任何个人和组织办理网络接入、域名注册、服务器托管、空间租用、内容分发、应用程序分发等服务，开设网络线路、电话线路，应当登记真实身份、装机地址、使用范围等信息，不得实施下列行为扰乱实名制管理:

（一）违反国家有关规定，将网络线路、电话线路出租他人使用的;

（二）未经变更登记，擅自改变网络线路、电话线路装机地址的;

（三）其他扰乱网络线路、电话线路实名制管理的行为。

第十四条 任何个人和组织不得非法制作、销售、提供、使用具有下列功能的设备、软件、工具、服务:

（一）具有使目标电话号码无法正常使用的自动追呼功能的;

（二）具有批量控制移动电话卡的功能的;

（三）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;

（四）具有批量网络地址自动切换，批量接收、提供短信验证、语音验证功能的;

（五）具有搜取移动终端用户信息，强行向不特定用户手机

发送、拦截短信息等功能的;

（六）其他由省级以上公安机关会同电信、广播电视等主管部门认定的，专门用于实施网络违法犯罪或者具有规避监管制度功能的设备、软件、工具、服务。

第十五条 任何个人和组织制作、销售、提供具有下列功能的设备、软件、工具、服务的，应当到公安机关、电信等主管部门备案，并登记购买者、使用者的真实身份信息:

（一）具有批量控制网络账号、上网线路、智能终端等功能的;

（二）具有网络虚拟定位功能的;

（三）具有侵入、控制计算机信息系统功能的;

（四）其他由省级以上公安机关会同电信等主管部门认定的，可能被大量用于网络违法犯罪的设备、软件、工具、服务。

前款所称的备案制度，由国务院公安部门会同电信等主管部门作具体规定。

第十六条 电信、金融、互联网等服务提供者应当按照法律法规和有关主管部门的规定，建立动态身份核验制度，对移动电话卡、物联网卡、银行账户、支付账户、网络账号使用者的真实身份进行动态核验。

在网络犯罪高发地区、期间，应当按照有关主管部门的要求增加动态身份核验的频次；发现移动电话卡、物联网卡、银行账户、支付账户、网络账号存在异常操作等情况下，应当及时进行动态身份核验。身份核验未通过的，应当采取限制、暂停、终止相关服务

等措施。

对限制、暂停或者终止相关服务，有关个人、组织提出异议的，电信、金融、互联网等服务提供者应当及时核查，核查通过的，应当恢复相关服务。

第十七条 国家建设、提供网络身份认证公共服务，电信、金融、互联网等服务提供者登记、核验用户真实身份，可以通过国家网络身份认证公共服务进行。

对存在网络犯罪风险的移动电话卡、物联网卡、银行账户、支付账户、网络账号，以及被用于实施网络犯罪的网络应用服务，相关行业主管部门可以要求电信、金融、互联网等服务提供者通过国家网络身份认证公共服务等方式对用户身份重新进行核验。

任何个人和组织不得破坏、干扰国家网络身份认证公共服务的运行。

第十八条 电信、金融、互联网等服务提供者对个人、组织申请办理移动电话卡、银行账户、支付账户、网络账号的，应当依照国家有关规定设定数量上限。

第三章 网络犯罪生态治理

第十九条 任何个人和组织不得明知他人利用网络实施违法犯罪，而为其提供互联网接入、云计算服务、算力归集和租赁、服务器托管、网络存储、通讯传输、域名解析、内容分发、开发运维、

广告推广、支付结算等支持和帮助。

第二十条 任何个人和组织不得明知他人利用网络实施违法犯罪，而为其提供或者变相提供经济支持:

（一）在他人设立的非法支付平台上流转资金的;

（二）在他人设立的淫秽、赌博等违法网站上投放广告推广信息的;

（三）其他为他人利用网络实施违法犯罪提供或者变相提供经济支持的。

第二十一条 任何个人和组织不得明知是他人网络违法犯罪所得的资金、数据、网络虚拟财产等而予以窝藏、转移、收购、代为销售或者以其他方法掩饰、隐瞒。

第二十二条 任何个人和组织不得从事下列侵犯公民个人信息或者危害数据安全的行为:

（一）非法收集、存储、使用、加工、传输、提供、公开、删除个人信息或者数据的;

（二）明知他人从事违法犯罪活动而为其提供个人信息或者数据支持的。

第二十三条 任何个人和组织不得明知他人利用网络实施违法犯罪，而为其提供人员招募、教育培训、证件办理等帮助。

第二十四条 任何个人和组织不得违反国家有关规定，实施网络产品安全漏洞发现、收集、发布等违法犯罪活动，或者散布、传播重要信息系统的设计方案、网络拓扑、核心源代码等可能危害网

络安全的信息。

第二十五条 未经省级以上网信部门、公安机关批准或者行业主管部门、运营者授权，任何个人、组织不得对网络安全等级保护第三级（含）以上的网络开展网络安全漏洞探测、渗透性测试等可能影响网络安全的活动。

未经设区的市级以上网信部门、公安机关批准或者行业主管部门、运营者授权，任何个人、组织不得对网络安全等级保护第二级（含）以下的网络开展网络安全漏洞探测、渗透性测试等可能影响网络安全的活动。

依法或者经批准、授权开展的，应当在活动实施五个工作日前向县级以上公安机关报告。法律、行政法规另有规定的，从其规定。

第二十六条 任何个人和组织不得明知是他人违法犯罪所得的资金，实施下列资金流转、支付结算等行为：

（一）为他人提供取款、转移运送现金等服务的；

（二）利用银行账户、支付账户或者网络交易、网络充值等平台，通过虚假交易等方式实施非法资金转移的；

（三）利用虚拟货币、其他网络虚拟财产为他人提供资金流转服务的。

第二十七条 任何个人和组织不得为他人有偿提供信息删除或者实际达到删除效果的屏蔽、替换、下沉信息等服务。互联网服务提供者及其从业人员不得在他人依法申请删除违法信息时，收取或者变相收取费用。

第二十八条 任何个人和组织不得通过下列方式发布信息，扰乱网络秩序:

（一）发布虚假信息的;

（二）通过控制计算机信息系统等违法方式发布信息的;

（三）控制大量非本人注册的网络账号发布信息，或者使用批量控制软件等提供虚假的评论、转发、点赞等服务的;

（四）发布违背社会公序良俗等信息，获取流量收益、广告收益的;

（五）其他实施流量造假，扰乱网络秩序等行为。

第二十九条 任何个人和组织在互联网上投放广告推广类信息或者提供广告推广中介等服务的，应当遵守以下规定:

（一）所投放的信息属于网络广告的，应当遵守网络广告法律法规; 所投放的信息不属于网络广告的，信息投放者、中介服务者应当核验交易对方的真实身份;

（二）核验所投放信息的网站、应用程序是否依法备案或者取得许可;

（三）检查网站、应用程序是否为淫秽、赌博、销售违禁品等明显违法的网站、应用程序;

（四）利用网站、应用程序、网络账号、通讯群组等帮助他人投放信息的，应当检查所投放的信息是否属于淫秽、赌博、销售违禁品等违法信息。

第三十条 任何个人和组织不得实施下列行为，为网络犯罪

提供吸引流量等帮助:

（一）明知他人利用网络实施违法犯罪，引导或者欺骗用户实施添加即时通信好友、关注社交平台账号、加入通信群组、下载应用程序等操作的;

（二）未经实名变更登记并公示，或者明知被用于违法犯罪而转让公众号、通信群组、论坛等管理权限的;

（三）其他明知他人利用网络实施违法犯罪仍为其提供吸引流量等帮助的行为。

第三十一条 任何个人和组织不得实施下列行为，非法推广相关应用程序、软件:

（一）为违法的应用程序提供电子签名、制作、封装、发布或者以测试为名提供下载等服务的;

（二）植入用户无法卸载的非基本功能软件，或者未经用户同意强行植入软件的;

（三）明知他人非法植入软件而为其提供推广服务的。

第三十二条 任何个人和组织不得未经互联网服务提供者授权，开发、销售、提供附加于其服务并影响服务正常运行或者损害用户公平交易的客户端软件或者服务平台。

第三十三条 任何个人和组织不得实施下列行为，破坏网络正常经营秩序:

（一）通过虚构交易、编造用户评价等方式进行虚假或者引人误解的商业宣传，或者损害他人商业信誉、商品声誉，干扰网络交

易正常进行的;

（二）通过虚构交易、虚构客户等非正常方式，骗领网络优惠券、补贴资金等的;

（三）其他破坏网络正常经营秩序的行为。

第四章 网络犯罪防治义务

第三十四条 国家机关、社会团体、企事业单位应当依照本法和有关法律法规的规定，履行预防、遏制、治理网络犯罪的义务。

履行网络犯罪防治义务的具体要求，由法律、行政法规或者国家标准的强制性要求作出规定。相关国家标准由国务院公安部门、国家网信部门、国务院标准化行政主管部门会同行业主管部门等制定。

第三十五条 网络运营者应当采取下列必要措施，保障其提供的服务免受违法犯罪侵害或者被用于实施违法犯罪活动:

（一）设立专门机构或者指定专门人员直接负责网络犯罪防治工作，网络运营者负责人为第一责任人;

（二）建立网络犯罪防治管理制度、操作规程，采取必要技术措施，并定期开展内部网络犯罪防治培训;

（三）建立网络犯罪防治工作预案，并定期开展应急处置演练;

（四）加强对第三方供应链单位以及参与网络运维重要岗位人员的管理，采取必要措施加强网络和数据安全监测预警;

（五）发现网络攻击威胁和网络违法犯罪线索的，应当及时采取处置措施，保存相关记录并向公安机关报告，配合开展侦查调查；

（六）其他必要的网络犯罪防治措施。

第三十六条 互联网接入服务提供者应当采取下列措施，防范其服务被用于实施违法犯罪活动：

（一）发现、阻断违反国家有关规定的网站、网络地址、应用程序；

（二）发现、阻断干扰、侵入、攻击、破坏网络服务设施等危害网络安全的行为；

（三）及时处置有关主管部门通报的利用其服务实施违法犯罪活动的行为。

第三十七条 电信服务提供者应当采取下列措施，防范其服务被用于实施违法犯罪活动：

（一）发现、阻断伪基站、违规开设或者租用网络线路、电话线路、擅自改变装机地址、擅自改变网络服务范围、将物联网卡用于非物联网应用等行为；

（二）发现、阻断为违法犯罪活动架设通信线路，提供设备运维、增强信号等行为；

（三）及时处置有关主管部门通报的利用其服务实施违法犯罪活动的行为。

第三十八条 电信、金融、互联网等服务提供者应当采取必

要措施，监测发现违反国家有关规定的异常注册、控制、使用移动电话卡、物联网卡、电话线路、银行账户、支付账户、网络账号、网络线路等行为，并及时阻断、处置相关卡、号、线路被用于实施网络违法犯罪活动。

对涉嫌用于实施网络违法犯罪活动的相关卡、号、线路，公安机关可以要求有关服务提供者停止提供服务。对被害人报案，申请资金紧急止付的，公安机关可以按照国家有关规定，作出紧急止付、快速冻结、资金返还等决定，金融服务提供者应当予以配合。

第三十九条 提供域名注册、主机托管、内容分发等服务的服务提供者，应当采取下列网络犯罪防治措施:

（一）提供域名注册服务的，应当采取监测发现、阻断、处置恶意注册、仿冒域名的措施，以及对用于实施违法犯罪活动域名的处置措施;

（二）提供服务器托管、空间租用、云服务的，应当采取监测发现、阻断、处置违法信息、网站、应用程序，拒绝服务攻击、恶意代码、僵尸网络，非法设立的虚拟专用网络等措施;

（三）提供内容分发服务的，应当采取监测发现、阻断、处置违法信息、网站、应用程序的措施。

第四十条 互联网服务提供者应当根据其提供的服务类别，采取下列网络犯罪防治措施:

（一）提供信息发布服务的，应当采取监测发现、防范、阻断、

处置违法信息，以及虚构转发、评论、点赞或者大量使用非本人注册账号发布信息的措施；

（二）提供网络交易服务的，应当采取监测发现、防范、阻断、处置销售或者拼装违禁物品、管制物品以及虚假交易等违法、可疑交易行为的措施；

（三）提供网络支付服务的，应当采取监测发现、防范、阻断、处置支付金额明显异常、账号使用频率异常等为违法、异常交易提供网络支付结算服务的措施；

（四）提供广告推广服务的，应当采取监测发现、防范、阻断、处置为违法犯罪活动提供广告推广，或者在广告服务中植入恶意代码、插入违法信息等的措施；

（五）提供信息搜索服务的，应当采取监测发现、防范、阻断、处置违法信息传播、推广的措施；提供付费信息搜索服务的，应当依法核验客户资质，明确付费搜索信息页面比例上限，并对付费搜索信息加注显著标识；

（六）提供网络游戏服务的，应当采取监测发现、防范、阻断、处置违法信息传播，变相从事赌博活动，网络虚拟财产异常、可疑变动情况的措施；

（七）提供应用程序分发服务的，应当采取监测发现、防范、阻断、处置专门用于侵入、非法控制计算机信息系统的程序、工具，未经许可、备案或者非法处理个人信息等违法违规应用程序的措施；

（八）提供数据调用接口服务的，应当建立身份认证、权限鉴别等技术措施，采取监测发现、防范、阻断、处置违法违规调用数据的措施；

（九）提供区块链服务的，应当采取监测发现、防范、阻断、处置在区块链上发布、传播违法信息、病毒木马、恶意程序或者为违法犯罪活动提供支付结算等帮助的措施；

（十）提供人工智能生成合成服务的，应当采取监测发现、防范、阻断、处置利用其服务制造、传播谣言等违法信息、实施侮辱、诽谤等违法犯罪活动的措施。

第四十一条 互联网信息服务提供者、移动智能终端生产者应当采取措施监测发现人工智能生成合成的信息，发现相关信息未添加标识的，应当及时采取消除等处置措施，或者添加标识提示用户该信息属于生成合成信息。

第四十二条 网络运营者在新技术新应用上线运营等重点环节，应当建立网络犯罪风险评估制度，防范新技术新应用被用于实施违法犯罪活动。

人工智能服务提供者应当采取措施，监测发现、防范、阻断、处置用户利用其服务实施违法犯罪活动、批量生成恶意代码等异常行为，保存有关记录并向公安机关等主管部门报告。

第四十三条 网络运营者、数据处理者应当履行网络和数据安全保护义务，建立健全网络和数据安全管理制度，采取技术措施及其他必要措施，防范其网络服务、数据被用于实施违法犯罪活动。

重要数据处理者应当建立数据标签标识等技术措施，监测、识别重要数据在不同主体之间传递的溯源链条。

第四十四条 国家网信部门统筹相关部门和网络运营者采取技术措施和其他必要措施，阻断来源于中华人民共和国境外的违法信息。

网络运营者发现用于实施违法犯罪活动的网络域名、网络地址、网络账号、电话线路、网络线路、应用程序，应当及时采取措施予以阻断，并向公安机关等主管部门报告。

任何个人和组织不得违反国家有关规定，制作、销售、提供相关设备、软件、工具、线路、服务，为他人获取、传播第一款被依法阻断的信息提供技术支持或者帮助。

第四十五条 以营利为目的，提供漏洞探测、渗透性测试等服务的机构，应当向设区的市级以上公安机关备案。

上述机构应当采取措施，加强对相关从业人员的培训和管理。

第四十六条 网络安全产品、服务提供者应当采取下列措施，防范其产品、服务被用于实施违法犯罪活动:

（一）向设区的市级以上公安机关报备本单位用于网络漏洞探测、渗透性测试的 IP 地址、域名等;

（二）提供众测平台服务的，应当核验相关授权证明文件;

（三）及时向公安机关、网信部门报告重大威胁情报和程序样本。

第四十七条 网站和应用程序的名称不得含有下列内容:

（一）法律、行政法规禁止发布或传输的信息;

（二）冒用或者未授权使用、关联使用党政机关、企事业单位等组织机构或者社会知名人士的名义，可能对公众造成欺骗或者误导的;

（三）其他经省级以上有关主管部门认定的不宜使用的名称。

第四十八条 省级以上公安机关、网信部门等有关主管部门可以对网络暴力事件的受害者发布网络保护令。

网络运营者应当按照网络保护令的要求，采取技术措施等必要措施，及时处置网络暴力事件，阻断有关网络暴力信息的传播。

第四十九条 设区的市级以上公安机关可以对网络暴力的实施者发布告诫书，责令其停止实施网络暴力行为。

第五十条 任何个人和组织不得实施下列侵害未成年人合法权益、损害未成年人身心健康的行为:

（一）利用网络组织、引诱、教唆、欺骗、强迫、帮助未成年人实施违法犯罪活动的;

（二）利用网络对未成年人实施威胁、侮辱、诽谤或者恶意损害形象等欺凌行为的;

（三）制作、复制、发布、传播或者持有涉及未成年人的淫秽色情信息的;

（四）泄露应当封存的未成年人犯罪记录或者可识别涉案未成年人身份的信息的;

（五）其他利用网络侵害未成年人合法权益，损害未成年人身

心健康的行为。

第五十一条 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、侦查犯罪以及防范、调查恐怖活动提供技术接口、解密等技术支持、协助与保障。具体要求由国务院公安部门会同有关部门制定。

公安机关、国家安全机关因维护国家安全、侦查犯罪的需要，可以依照国家有关规定，要求有关组织采取发现、防范危害国家安全和犯罪活动的管理措施和其他必要措施，有关组织应当予以配合。

第五章 跨境网络犯罪防治

第五十二条 公安机关和有关主管部门依照本法和有关法律法规，并根据国家缔结、参加的国际条约或者按照平等互惠原则，对在境外或者利用境外网络资源对中华人民共和国及其公民或者机构实施网络犯罪活动，或者我国公民在境外实施我国法律禁止的网络犯罪活动，开展网络犯罪防治国际执法合作。

第五十三条 境外个人和组织为中华人民共和国境内用户提供互联网服务及相关网络产品、服务，为网络犯罪活动提供支持和帮助的，国家网信部门可以依法对其采取技术阻断措施。

第五十四条 境外个人和组织利用网络向中华人民共和国境内实施诈骗、赌博、传播淫秽物品等犯罪活动的，对其犯罪所得

及利用犯罪所得投资的企业、有价证券、不动产等资产，应当依法查封、扣押、冻结；经人民法院审理，可以依法没收。有关主管部门可以作出限制其在境内直接或者间接投资的决定。

第五十五条 境外机构、组织、个人利用网络制造、传播虚假信息，损害中华人民共和国国家主权、安全、发展利益或者公共利益的，有关主管部门可以作出冻结财产、限制有关人员入境、限制在境内直接或者间接投资等决定。

第五十六条 对利用网络跨境实施本法第三章规定的行为，依法受到刑事处罚的中国公民，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，决定自处罚完毕后六个月至三年内不准其出境。

境外人员利用网络实施本法第三章规定的违法犯罪行为的，有关主管部门可以依法决定不准其入境。

第六章 法律责任

第五十七条 违反本法第十一条至十三条的规定，扰乱实名注册等制度的，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。

对上述被行政处罚的个人和组织，有关主管部门可以将其列入黑名单，责令有关服务提供者对其采取限制使用、限制或者禁

止开设卡号等惩戒措施。

第五十八条 违反本法第十四条、第十五条、第十七条第三款和第四十四条第三款规定，制作、销售、提供、使用相关设备、软件、工具、服务的，由公安机关、网信部门、电信主管部门、市场监管部门等依据职责予以没收，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。

第五十九条 违反本法第十九条至第三十三条规定，扰乱网络秩序的，由公安机关、网信部门、电信主管部门、金融、市场监管、文化和旅游等主管部门，依据职责责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销业务许可或者营业执照，并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。

第六十条 电信、金融、互联网等服务提供者有下列情形之一，由有关主管部门责令改正，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、吊销业务许可或者营业执照，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）违反本法第十六条、第十七条第一款、第二款的规定，

未落实实名注册等制度，依法核验用户真实身份的；

（二）违反本法第三十四条至第四十三条、第四十八条第二款的规定，未落实网络犯罪防治义务，依法采取相关监测发现、阻断处置的措施的；

（三）违反本法第四十五条至第四十六条的规定，未依法履行网络安全产品、服务备案等义务的；

（四）违反本法第四十七条的规定，未依法履行网站和应用程序名称管理义务的；

（五）违反本法第五十一条的规定，未依法提供技术支持、协助与保障的。

第六十一条 违反本法第五十条规定，侵害未成年人合法权益的，由公安机关处二十万元以下罚款；情节严重的，处五十万元以下或者违法所得十倍以下罚款，可以并处十五日以下拘留。

第六十二条 网信部门、电信主管部门、公安机关和其他有关部门对违反本法规定的行为依法给予的行政处罚，应当依照法律、行政法规的规定记入信用档案。

第六十三条 违反本法有关规定，扰乱实名注册等制度，扰乱网络秩序，不落实网络犯罪防治义务，导致他人被网络犯罪侵害造成损失的，按照其过错依法承担民事责任。

第六十四条 电信、金融、互联网等服务提供者者不履行本法规定的网络犯罪防治义务，侵害众多个人的合法权益，或者致使国家利益、社会公共利益受到损害的，人民检察院、有关主管

部门以及相关社会组织可以依法向人民法院提起公益诉讼。

第六十五条 网信部门、电信主管部门、公安机关和其他有关部门的工作人员玩忽职守、滥用职权、徇私舞弊或者利用职务上的便利索取、收受他人财物，尚不构成犯罪的，依法给予处分。

第六十六条 违反本法规定，构成违反治安管理行为的，由公安机关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

第六十七条 本法所称网络犯罪，是指针对或者主要利用网络实施的危害国家安全、公共安全、公民人身财产安全等犯罪。

第六十八条 本法自 XX 施行。

关于起草《网络犯罪防治法（征求意见稿）》的说明

针对当前严峻复杂的网络犯罪形势，公安部在前期充分调研的基础上，研究起草了《网络犯罪防治法（征求意见稿）》，重点从网络基础资源管理、网络犯罪生态治理、网络犯罪防治义务、跨境网络犯罪防治等方面，制定具体网络犯罪防范制度，着力构建打防结合、防范为先、源头治理、协同联动的网络犯罪防治格局。现将有关情况说明如下：

一、起草过程

随着互联网的快速发展，传统犯罪不断向网上蔓延。借助互联网跨地域、扁平化的特点，网络犯罪形成物料供应、技术支持、引流推广、支付结算等体系庞大、盘根错节的黑灰产业链条，各环节链条分工合作，高效完成网络犯罪。为此，仅靠个案打击、事后惩处不足以遏制高发频发的网络犯罪蔓延势头，必须坚持打防结合、防范为先，做到关口前移，强化行政监管，有效打击整治网络犯罪生态。

公安部会同相关部门深入调研网络犯罪形势、特点，结合网络犯罪打击整治中的难点问题，研究形成了《网络犯罪防治法（征求意见稿）》。期间，公安部多轮次征求相关部门意见，召开法律研讨会，邀请科研院所、互联网企业专家进行专题研讨，对《网

络犯罪防治法（征求意见稿）》进行修改完善。

二、总体考虑和主要内容

《网络犯罪防治法（征求意见稿）》共7章68条，针对当前网络犯罪的严峻态势，坚持“打防结合、防范为先、生态治理、协同联动”的原则，着力构建多部门联合、跨地域联动，政府、企业、网民共同参与的网络犯罪综合防治体系，力争做到网络犯罪发现在早、打击在小，有效遏制网络犯罪高发频发势头。

（一）明确网络基础资源管理制度。在《网络安全法》基础上进一步明确实名制等要求，规定任何个人、组织不得实施干扰、破坏实名制的行为，有效遏制网络犯罪“物料供应”黑灰产。对当前大量被网络犯罪及黑灰产使用的黑卡、黑号、黑线路、黑设备等加强行政监管，强化对网络异常行为的监测管控。

（二）明确网络犯罪生态治理制度。网络犯罪黑灰产与网络犯罪依附共生、利益共享，极大降低了网络犯罪门槛。由于缺乏明确法律依据，对黑灰产团伙往往难以依法治理。《网络犯罪防治法（征求意见稿）》立足网络犯罪黑灰产现状，对其中起到基础作用的网络支付、引流推广等黑灰产业链条予以法律规制，为打击治理网络犯罪生态提供进一步法律支撑。

（三）明确网络犯罪防治义务。按照网络服务提供者的业务规模、技术能力等设置相应的网络犯罪防治义务，督促其建立健全防范、发现网络犯罪的制度、措施，充分发挥网络服务提供者预防网络犯罪“第一道防线”的作用。推进实施可信数字身份战略，建

立、应用国家网络身份认证公共服务。

（四）明确跨境网络犯罪防治制度。针对网络犯罪跨国跨境的特点，《网络犯罪防治法（征求意见稿）》规定了跨国跨境网络犯罪防治措施，规定了跨境网络犯罪制裁、跨境网络服务监管、相关人员限制出入境等制度，为从源头治理、阻断跨境网络犯罪提供法律支撑。