**全国人大常委会｜关于检查《网络安全法》《关于加强网络信息保护的决定》实施情况的报告**

http://www.djbh.net/webdev/web/images/shang-1.jpg

来源：admin 发布日期：2018-01-03

**前哨按语**

2017年12月24日上午，第十二届全国人民代表大会常务委员会第三十一次会议全体会议，听取全国人大常委会执法检查组关于检查《中华人民共和国网络安全法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》实施情况的报告。《网络安全法》实施不满3个月即启动执法检查，这在全国人大常委会监督工作中尚属首次，以下是执法检查组的报告全文。

**全国人民代表大会常务委员会执法检查组关于检查《中华人民共和国网络安全法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》实施情况的报告**

**——2017年12月24日在第十二届全国人民代表大会常务委员会第三十一次会议上**

全国人大常委会副委员长　王胜俊

全国人民代表大会常务委员会：

　　网络安全事关党的长期执政，事关国家长治久安，事关经济社会发展和人民群众切身利益。习近平总书记强调指出，没有网络安全就没有国家安全，没有信息化就没有现代化。全国人大常委会高度重视网络安全工作，2012年12月审议通过《全国人民代表大会常务委员会关于加强网络信息保护的决定》，2016年11月审议通过《中华人民共和国网络安全法》(以下简称**“一法一决定”**)。根据2017年监督工作计划，全国人大常委会执法检查组于2017年8月至10月对“一法一决定”的实施情况进行了检查。现在，我代表执法检查组向常委会作报告。

**一、执法检查的工作情况**

　　网络安全法是今年6月1日开始施行的。**一部新制定的法律实施不满3个月即启动执法检查，这在全国人大常委会监督工作中尚属首次。**张德江委员长十分重视这次执法检查，作了重要批示，指出：网络安全事关国家长治久安，事关经济社会发展和人民群众福祉。全国人大常委会在网络安全法实施当年就开展执法检查，要贯彻落实习近平总书记关于“要树立正确的网络安全观”的重要指示精神，督促有关方面进一步加强法律宣传，增强全社会网络安全意识，抓紧配套法规政策制定，确保法律有效实施，着力提升网络空间治理水平，切实维护国家网络空间安全和人民群众合法权益。希望检查组精心组织好这次执法检查，坚持问题导向，务求取得实效。根据张德江委员长的批示精神，内务司法委员会、财政经济委员会、教育科学文化卫生委员会和常委会办公厅等单位反复研究，确定了这次**执法检查的五个重点：一是开展法律宣传教育的情况；二是制定配套法规规章的情况；三是强化关键信息基础设施保护及落实网络安全等级保护制度的情况；四是治理网络违法违规信息，维护网络空间良好生态的情况；五是落实公民个人信息保护制度，查处侵犯公民个人信息及相关违法犯罪的情况。**

　　8月25日，执法检查组召开第一次全体会议，传达张德江委员长的重要批示。会议听取了国家互联网信息办公室、工业和信息化部、公安部、国家新闻出版广电总局、最高人民法院关于“一法一决定”贯彻实施情况的汇报，教育部、科技部、交通运输部等单位提交了书面汇报材料。

　　根据安排，王晨副委员长兼秘书长、沈跃跃、张平、万鄂湘、陈竺副委员长和我六位副委员长参加这次执法检查。检查组赴内蒙古、黑龙江、福建、河南、广东、重庆等6省（区、市）进行检查，期间，检查组听取了有关省、市、县政府的汇报，先后召开30余次座谈会，实地考察了部分网络安全指挥平台和关键信息基础设施运营单位。另外，还委托12个省（区、市）人大常委会对本行政区域“一法一决定”实施情况进行检查。

　　为了深入了解“一法一决定”实施情况，这次执法检查在方式方法上作了一些**新的尝试**：**一是请第三方专业机构参与**。9月上旬至10月中旬，检查组在实地检查的6个省（区、市）各选取20个重要信息系统，委托中国信息安全测评中心进行漏洞扫描和模拟攻击，并就所检测系统的网络安全情况出具专业检测报告。检查组还委托中国青年报社社会调查中心就“一法一决定”中与公众关系密切的10个方面的问题，在全国31个省（区、市）进行了民意调查，出具了调查报告。共有10370人参与这次调查。第三方机构的有序参与，增强了本次检查的专业性、权威性和客观公正性。**二是专家参与。**考虑到网络安全专业性较强，执法检查期间，检查组先后从国家信息技术安全研究中心等单位聘请21名网络安全专家和长期从事网络安全工作的专业技术人员参加检查，为检查组提供技术支持，增强检查的针对性和实效性。**三是随机抽查。**各检查小组均按检查方案要求，随机选取若干关键信息基础设施运营单位，在不打招呼的情况下进行临时抽查。6个检查小组共对13个单位进行了随机抽查。远程检测的120个重要信息系统也均由执法检查组随机选取，在运营单位不知情的情况下完成检测。

**二、贯彻实施“一法一决定”的做法和成效**

　　近年来，各级党委政府认真组织学习习近平总书记系列重要讲话和关于网络安全的重要论述，深入贯彻中央关于“建设网络强国”的战略部署，把网络安全纳入经济社会发展全局来统筹谋划部署，大力推进网络安全和网络信息保护工作，法律实施取得了积极成效。

**（一）深入开展宣传教育，增强网络安全意识**

**一是把增强全民网络安全意识作为基础工程。**国家互联网信息办公室、工业和信息化部、公安部等9部门连续四年组织开展网络安全周和主题日宣传活动，每年活动期间组织的讲座论坛等都超过1万场次，年均覆盖人数约2亿人。网络安全法颁布后，各地均通过报刊杂志、电台电视台、门户网站、政务微信微博等，对法律核心内容进行宣传解读。**二是加强重点单位、重点行业法律宣传教育。**工业和信息化部将学习“一法一决定”情况纳入各基础电信运营企业的年度考核指标，并组织百度、阿里、腾讯等重点互联网企业开展学习。公安部组织全国公安机关、200多个中央部委和中央企业、260多家信息安全企业相关人员进行集中学习。国家新闻出版广电总局组织开展了网络安全知识技能练兵和竞赛活动。内蒙古、黑龙江等省(区)对重点单位、重点行业负责网络安全的业务骨干进行了重点培训。**三是紧紧抓住领导干部这个关键少数，把提升领导干部的网络安全意识作为重中之重。**广东、福建等地通过举办领导干部网络安全和信息化专题研讨班等形式，推动领导干部率先知法懂法用法。交通运输部党组成员带头学习，并举办了“交通运输网络安全局级领导专题培训班”，教育部举办了教育系统网络安全培训班，对各省级教育行政部门、直属高校、部直属机关负责人进行专题培训。**四是加强重点人群宣传教育。**各地把青少年网民作为普法重点，开展了“网络安全进校园、进家庭”、“争做四有好网民”等活动，引导广大青少年依法、文明、健康上网。

**（二）制定配套法规政策，构建网络安全制度体系**

　　为配合“一法一决定”实施，近年来，国务院相关部门出台了**《国家网络空间安全战略》《通信网络安全防护管理办法》《电信和互联网用户个人信息保护规定》《电话用户真实身份信息登记规定》《新闻出版广播影视网络安全管理办法》《公共互联网网络安全突发事件应急预案》等配套规章、规划和政策文件**。国家互联网信息办公室会同有关部门出台了**《关于加强国家网络安全标准化工作的若干意见》**，加快了网络安全国家标准制定工作，目前已发布198项网络安全国家标准。最高法院、最高检察院出台了**《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》**。一些省份也开展了配套法规立法工作，内蒙古自治区人大常委会制定了《计算机信息系统安全保护办法》，福建省人大常委会通过了《福建省电信设施建设与保护条例》，广东省人大常委会出台了《关于落实电信用户真实身份信息登记制度的决定》，黑龙江省人大常委会制定了《工业信息安全管理条例》。重庆市坚持网络安全与信息化发展并重，加强电子政务制度建设，完善了政府网站管理制度。一系列配套法规、规章和政策文件出台，助推了“一法一决定”的贯彻实施。

**（三）提升安全防范能力，着力保障网络运行安全**

**一是强化关键信息基础设施防护。**2016年，国家互联网信息办公室等部门组织开展了关键信息基础设施摸底排查工作，对1.1万个重要信息系统安全运行状况进行抽查和技术检测，完成了对金融、能源、通信、交通、广电、教育、医疗、社保等多个重点行业的网络安全风险评估，提出整改建议4000余条。**二是开展网络基础设施防护工作。**工业和信息化部开展了网络基础设施摸底工作，全面梳理网络设施和信息系统，目前全行业共确定关键网络设施和重要信息系统11590个。2017年以来，监督抽查重点网络系统和工业控制系统900余个，通知整改漏洞78980个。**三是深入推进网络安全等级保护。**已累计受理备案14万个信息系统，其中三级以上重要信息系统1.7万个，基本涵盖了所有关键信息基础设施。同时，对纳入等级保护的信息系统开展常态化检查，近年来累计发现整改各类安全漏洞近40万个。**四是建立通报预警机制。**公安部牵头建立了国家网络安全通报预警机制，通报范围已覆盖100个中央党政军机构、101家央企、31个省(区、市)和新疆生产建设兵团，各地也都建立了网络安全与信息安全通报机制，实时通报处置各类隐患漏洞。教育部建立了教育系统重要网站和信息系统安全监测预警机制，已累计通报处置安全威胁3.5万个。**五是积极开展网络安全协调联动平台建设。**国家互联网信息办公室牵头建立了关键信息基础设施应急技术支持和协助机制，不断提升关键信息基础设施整体应急反应能力、安全保障能力和协调联动能力。**六是大力开展网络安全专项整治工作。**公安部会同有关单位组织开展了大型互联网企业专项保卫行动、网站安全和互联网电子邮件安全专项整治行动，发现整改了一批网络安全深层次问题和隐患。

**（四）治理违法违规信息，维护网络空间清朗**

　　各地各有关部门认真落实法律要求，扎实做好网络意识形态工作，坚决清理各类违法违规信息。**通过开展“扫黄打非”、“剑网”等系列行动，对互联网站、应用程序、论坛、博客、微博、公众账号、即时通讯工具、网络直播中宣扬恐怖暴力、淫秽色情等信息及时清理。**2015年以来，国家互联网信息办公室等部门依法约谈违法违规网站2200余家，取消违法违规网站许可或备案、关停违法网站13000多家，有关网站按照用户服务协议关闭违法违规账号近1000万个，对网上各类违法行为形成有力震慑。中国青年报社社会调查中心提供给检查组的万人调查分析报告(以下简称“万人调查报告”)显示，在参与调查的10370人中，超过90%的受访者对治理成效给予肯定，其中有63.5%的人认为近年来网络上危害国家安全、宣扬恐怖暴力、淫秽色情等违法违规信息明显减少。法律实施主管部门还建立了网络信息巡查机制和公众举报平台，及时清理违法违规信息。重庆等地重视加强网络内容建设，积极创作优秀网络作品，做强网上正面宣传。

**（五）加强个人信息保护，打击侵犯用户信息安全违法犯罪**

**全面落实网络接入(网站备案和域名／IP地址)、固定电话、移动电话实名制**办理要求，凡用户不提供真实信息的，运营者不再为其提供相关服务。五年来，组织电信企业对3亿多未实名的老用户进行补登记，对拒不补登记的1000余万用户依法暂停提供服务。为确保用户信息安全，有关部门指导各网络运营单位进一步强化了内控管理制度，要求对批量导出、复制、销毁信息等重大操作的申请、使用和有效期实行严格管理，从工作流程上防止用户信息的批量泄露。河南省加强对保存用户信息关键系统的安全防护，提升防止黑客攻击能力。针对侵犯用户个人信息犯罪高发态势，**公安部部署开展专项打击行动**，在31个省(区、市)和新疆生产建设兵团公安机关建立了反诈骗中心，**统筹协调打击利用公民个人信息实施的电信网络诈骗犯罪**，近两年，共侦破侵犯个人信息犯罪相关案件3700余起，抓获犯罪嫌疑人11000余名。2014年至2017年9月，全国法院共审理利用网络侵犯公民个人信息犯罪案件1529件，取得了较好的法律效果和社会效果。

**（六）加大支持力度，推进网络安全核心技术创新**

　　为落实网络安全法“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利用”等要求，**科技部会同国家互联网信息办公室共同编制了专项研究计划**，立足网络空间安全发展现状，围绕提高我国关键信息基础设施和数据安全的防护能力、支撑网络空间可信管理和数字资产保护、提升网络空间防护能力等目标，确立若干重点研究方向。为了加大对网络安全技术研究开发和应用的支持，科技部、工业和信息化部等部门，在“十三五”国家重点研发计划中优先启动了**“网络空间安全重点专项”**，投入国拨经费13.84亿元，系统部署了47项研究任务，力争到2020年，基本形成自主可控的网络空间安全核心技术体系。另外，在**“科技创新2030——重大项目”**中，也将优先安排一批网络空间安全重大研究项目，为提升我国信息监管、泄密窃密防范、网络防御等提供技术支持。教育部创新网络安全人才培养模式，增设了网络空间安全一级学科，与有关部门共同下发了**《关于加强网络安全学科建设和人才培养的意见》**，启动了一流网络安全学院建设示范项目，为网络安全技术创新提供人才支持。

**三、工作中存在的困难和问题**

　　从检查情况看，各地在贯彻实施“一法一决定”、维护网络安全方面还存在一些困难和问题。

**（一）网络安全意识亟待增强**

　　许多关键信息基础设施运营单位对网络安全的重要性认识不到位，认为受到网络攻击只是小概率事件，对可能受到的网络攻击的危害性缺乏认知。在信息化方面**“重建设、轻安全；重使用、轻防护”**，缺乏主动防御意识，不愿在安全防护方面进行必要投入；在处理业务信息系统可用性和安全性的关系时，往往更重视可用性，在二者有冲突时，往往会降低安全性要求。不少地方政府和部门领导干部不能从国家安全的高度认识网络安全，没有把网络安全工作列入本级政府和部门工作重要议程，或者只是口头上重视，**“说起来重要，干起来次要，忙起来不要”**。社会公众网络安全意识总体不强，“万人调查报告”显示，有55.4%的受访者认为，他们身边的许多人缺乏网络安全意识，对网络安全“知其然不知其所以然”。

**（二）网络安全基础建设总体薄弱**

**一是网络安全态势感知平台建设滞后。**网络安全风险具有很强的隐蔽性，感知安全态势是做好网络安全最基本最基础的工作。维护网络安全，首先要知道风险在哪里，是什么样的风险，什么时候发生风险。但不少省份尚未启动网络安全态势感知平台建设，不能实现对重要信息系统网络安全风险的全天候实时、动态监测。**二是容灾备份体系建设总体滞后。**不少关系国计民生的关键信息基础设施运营单位没有按照法律规定对重要数据进行异地容灾备份，而仅仅采取了一些简单的数据备份措施，有的甚至尚未进行过容灾备份，不能有效应对重大网络安全风险。在有些省份，多数重要信息系统未按法律要求进行异地容灾备份。**三是重要工业控制企业的设备和控制系统国产化程度有待提高。**一些重要工控企业对外国技术依赖严重，不仅生产控制系统由国外公司建设，配套的网络及安全设备也采用国外产品，网络及安全设备的配置由外方人员操控，企业内部人员甚至不掌握安全设备配置和管理权限。在有的省份，重要工控企业的生产控制系统国产化率不足20%。**四是应急预案流于形式。**有的网络安全应急预案侧重于设备设施障碍的排除，针对网络攻击、信息泄露等网络空间安全事件的内容较少；有的应急预案缺乏可操作性；有的应急预案长期未修订，已不能应对当下的网络安全事件；许多单位由于应急演练相关条件不足，未真正举行过应急演练；不少地方和行业用于解决网络安全问题的经费不足，发现了问题后，往往因经费缺乏不能及时解决。

**（三）网络安全风险和隐患突出**

　　为了解网络运行情况，执法检查组委托**中国信息安全测评中心对随机选取的120个关键信息基础设施(60个门户网站和60个业务系统)进行了远程渗透测试和漏洞扫描**。该中心出具的报告显示，本次远程测试的120个关键信息基础设施中，共存在30个安全漏洞，包括高危漏洞13个，其中某省级部门互联网监管综合平台存在越权上传、越权下载、越权删除文件等3个高危漏洞，严重威胁了系统及服务器安全，也存在严重的用户信息泄露风险。远程检测还发现，多个设区的市政府门户网站存在页面被篡改风险。执法检查组现场抽查时发现，许多单位没有依照法律规定留存网络日志，这可能导致发生网络安全事件时无法及时进行追溯和处置；有的单位从未对重要信息系统进行风险评估，对可能面临的网络安全态势缺乏认知。检查还发现，在许多单位，内网和专网安全建设没有引起足够重视，有的单位对内网系统未部署任何安全防护设施，长期不进行漏洞扫描，存在重大网络安全隐患。随着各地区各领域信息化建设的推进，各行业各领域数据化、在线化、远程化趋势更加明显，对网络安全提出了更高要求。

**（四）用户个人信息保护工作形势严峻**

　　“万人调查报告”显示，“一法一决定”关于用户个人信息保护的多项制度落实得并不理想：有52.1%的受访者认为，法律关于“网络服务提供者和其他企业事业单位在业务活动中收集、使用公民个人电子信息，必须明示收集、使用信息的目的、方式和范围”的规定执行得不好或者一般；有49.6%的受访者曾遇到过度收集用户信息现象，其中18.3%的受访者经常遇到过度采集用户信息现象；有61.2%的人遇到过有关企业利用自己的优势地位强制收集、使用用户信息，如果不接受就不能使用该产品或接受服务的“霸王条款”；有52.5%的人认为执法部门保护用户信息的成效一般或者不好，不少人反映，在发现本人信息被泄露或者被滥用后，举报难、投诉难、立案难现象比较普遍。许多受访者反映，当前免费应用程序普遍存在过度收集用户信息、侵犯个人隐私问题，但几乎没有受到任何监管和依法惩处。检查发现，**有的互联网公司和公共服务部门存储了大量公民个人信息，但安防技术严重滞后，容易被不法分子窃取和盗用。**一些单位内控制度不完善或不落实，少数“内鬼”为牟取不法利益铤而走险，致使用户信息大批量泄露。当前在一些地方，利用网络非法采集、窃取、贩卖和利用用户信息已形成黑色产业链。从公安部门近期破获的案件看，用户信息泄露呈现渠道多、窃取违法行为成本低、追查难度大等特点，而且违法分子使用的手段不断升级，因用户信息泄露引发的“精准诈骗”案件增多，给人民群众财产安全造成严重危害。

**（五）网络安全执法体制有待进一步理顺**

**网络安全监管“九龙治水”现象仍然存在，权责不清、各自为战、执法推诿、效率低下等问题尚未有效解决，**法律赋予网信部门的统筹协调职能履行不够顺畅。一些地方网络信息安全多头管理问题比较突出，但在发生信息泄露、滥用用户个人信息等信息安全事件后，用户又经常遇到投诉无门、部门之间推诿扯皮的问题。“万人调查报告”显示，有18.9%的受访者反映，在遇到网络安全问题后，他们不知该向哪个部门举报和投诉，即使举报了也往往不予处理或者没有结果。参加座谈的多数网络运营单位反映，行政执法过程中存在不同执法部门对同一单位、同一事项重复检查且检查标准不一等问题，不同法律实施主管机关采集的数据还不能实现“互联互通”，经常给网络运营商增加额外负担。不少人认为，如果不能合理定位，准确厘清部门之间的职责，等级保护制度和关键信息基础设施保护制度落实过程中也会产生执法不协调问题。另外，检查发现，城市轨道交通控制系统等工控系统网络安全管理责任边界不清，运营单位落实网络安全责任制存在困难；通信行业监管和行政执法力量严重不足，执法力量与当前网络安全事件频发多发的严峻形势不相适应。

**（六）网络安全法配套法规有待完善**

　　不少单位反映，作为网络安全管理方面的基础性法律，**网络安全法不少内容还只是原则性规定，真正“落地”还有赖于配套制度的完善。**比如，网络安全法虽然对数据安全和利用作了规定，但现实中数据运用比较复杂，**数据脱敏标准、企业间数据共享规则**等，仍然需要有关法规规章予以明确；网络安全法仅明确了关键信息基础设施运营者数据出境需进行评估，但其他网络运营者掌握的**重要数据出境**是否进行安全评估，尚待进一步明确。关键信息基础设施保护制度是网络安全法一项重要制度，但对于**什么是关键信息基础设施、关键信息基础设施认定的标准和程序**等，目前认识尚不一致，需要配套法规予以明确。**关键信息基础设施如何进行年度检测评估、网络运营者和管理部门如何统一发布网络安全预警信息、如何扶持网络安全自主知识产权**等，也有待于配套法规规章予以明确。

**（七）网络安全人才短缺**

　　参与调查的10370人中，有超过69%的受访者认为，所在单位或者熟悉的人中，能够熟练从事网络安全防护的专业技术人才较少，无法满足现实需要，其中有21.6%的受访者认为所在单位基本上无人熟悉网络安全防护技术。从检查的情况看，不管是经济发达地区还是相对落后地区，网络安全技术人才都比较匮乏，现有的网络运营单位技术人才多侧重于系统使用、操作维护，对网络安全风险的监控、应急处置和综合防护能力不足，难以适应保障网络安全的需要。有的关键信息基础设施核心业务系统虽然安装了防护系统，但由于缺乏高水平的安全技术人才，不能对安全软件进行升级和打补丁，从而使网络安全防护产品难以有效发挥作用。**不少政府门户网站没有专门的网络安全技术人才，网站管理人员没有接受过系统的网络安全技能培训。**另外，网络安全主管部门专业人才也明显不足。受到编制、职务、薪资等因素制约，许多地方网信、公安、通信管理、工信等单位往往招不到或留不住专业技术人才，一线执法人员的专业素养和技能难以胜任网络运行安全常态化监管执法职责。

**四、几点建议**

　　根据检查情况，检查组对进一步贯彻实施“一法一决定”提出以下建议。

**（一）进一步提高对网络安全重要性的认识**

　　在信息时代，网络空间已经成为继陆地、海洋、天空、外层空间之外，人类活动的第五空间，成为国家利益的新边疆和世界各主要国家战略博弈的新领域，网络安全对国家安全牵一发而动全身，已成为基础性、全局性的国家安全问题。党的十九大报告强调，**网络安全等非传统安全是人类面临的共同挑战之一**，要坚持总体国家安全观，以人民安全为宗旨，以政治安全为根本，统筹外部安全和内部安全、国土安全和国民安全、传统安全和非传统安全、自身安全和共同安全，完善国家安全制度体系，加强国家安全能力建设。要进一步深化对新形势下加强网络安全工作重要性的认识，**不断增强贯彻落实网络安全法等法律法规的紧迫感和自觉性**。法律实施主管机关和其他相关单位要结合工作实际，进一步加大对网络安全法的宣传培训力度，不仅让广大网络运营商、关键信息基础设施运营单位的相关人员能够熟知法律内容，还要以喜闻乐见的方式加强对社会公众的宣传，让广大公众认识到网络安全与自身的密切关系，增强全社会的网络安全意识。

**（二）正确处理安全和发展的关系**

　　习近平总书记强调指出，网络安全和信息化是相辅相成的。安全是发展的前提，发展是安全的保障，安全和发展要同步推进。要充分认识到互联网在国家管理、经济发展和社会治理中的作用，继续推进电子政务、电子商务、新型智慧型城市建设，不断推进技术融合、业务融合、数据融合，打通经济社会发展的信息“大动脉”。要按照**网络安全法“坚持网络安全与信息化发展并重”**的要求，坚持一手抓网络和信息化发展，一手抓网络安全，“两手抓，两手都要硬”。对于网络安全，既要重视传统的信息安全和意识形态安全，营造风清气正、正能量充沛的网络空间，也要高度重视攻防能力提升，有效防范网络攻击，切实维护网络信息系统安全。要科学制定不同行业、不同单位的网络安全标准，认真研究解决有些单位提出的“网络安全合规成本过高”的问题。鼓励和支持网络安全产业的发展，发挥社会力量的作用，提供安全的产品和服务。

**（三）加快完善网络安全法配套法规规章**

**要加快《关键信息基础设施安全保护条例》《网络安全等级保护条例》的立法进程**，对实践中大家普遍感觉难以把握的问题，如什么是关键信息基础设施、如何认定关键信息基础设施等作出明确规定，并对等级保护制度和关键信息基础设施保护制度落实过程中的部门职责进一步予以明确。网信、工信、公安等部门要尽快制定配套规章或者文件，**细化法律中个人信息和重要数据出境安全评估、网络数据管理、网络安全监测预警和信息通报、网络安全审查、网络安全认证和安全检测结果互认等制度**。此前已制定的一些行政法规和部门规章也应根据网络安全法的要求以及法律实施中遇到的新情况新问题，及时予以修改完善。根据防范和打击网络违法犯罪的需要，**加强互联网刑事立法，研究制定网络违法犯罪防治法，推动网络违法犯罪行政处罚与刑事处罚的有效衔接。**

**（四）着力提升网络安全防护能力**

**一是加快网络安全态势感知平台建设。**要整合各部门资源，建立统一的全天候网络安全感知平台，以更好地发现风险、感知风险，进而**构建统一高效的网络安全风险发现机制、报告机制、情报共享机制、研判处置机制**，准确把握网络安全风险发生的规律、动向、趋势。**二是依法组织开展风险评估。**要尽快完善网络安全风险评估机制，加强对金融、能源、交通等重要行业和领域的评估，根据评估情况，适时调整网络安全工作方案和保护措施。**三是定期组织应急演练。**组织关键信息基础设施运营单位定期进行应急演练，使事关国家安全、关系国计民生的重要信息系统能够有效应对有组织的高强度网络攻击。**四是要认真落实法律要求，加快关键信息基础设施数据的容灾备份建设，并定期开展灾备效果验证，提升信息系统的抗灾、减灾和恢复能力。**要督促网络运营单位认真落实法律规定，依法留存网络日志。**五是要加强网络安全保密保障体系建设**，提升网络安全保密装备能力，推进网络安全保密技术保障基础设施建设。**六是要大力推进国产化替代工程。**加大技术研发力度，逐步提高重要工业企业信息控制系统的国产化率，提升关键信息基础设施和网络安全设备的自主可控能力。

**（五）进一步加大用户个人信息保护力度**

**一是要加快个人信息保护法立法进程。**通过专门立法，明确网络运营者收集用户信息的原则、程序，明确其对收集到的信息的保密和保护义务，不当使用、保护不力应当承担的责任，以及监督检查和评估措施。**二是加强安全防护。**强化数据安全监管手段建设，实施数据资源分级分类管理，推动大数据场景下的数据防窃密、防篡改、防泄露等安全技术的研发和部署。**三是要认真研究用户实名制的范围和方式**，坚决避免信息采集主体过多、实名登记事项过滥问题。各地区各单位对某一事项实施实名登记制度，应当有明确的法律依据。要改进实名信息采集方式，减少实名信息采集的内容。**四是加大监督检查力度。**建立第三方评估机制，督促网络运营和公共服务单位严格依法收集用户信息，建立健全内部管理制度，有效降低“内鬼”窃密风险。**五是进一步加大打击力度。**公安机关要加大对网络攻击、网络诈骗、网络有害信息等违法犯罪活动的打击力度，切断网络犯罪利益链条，持续形成高压态势，落实法律保护公民个人信息的规定，使广大公民的合法权益免受侵害。**六是要完善投诉受理机制。**研究建立统一高效的用户信息安全事件投诉受理机制，为用户投诉、举报提供便利，维护人民群众合法权益。

**（六）强化网络安全工作统筹协调**

　　网络安全工作涉及领域多、范围广、任务重、难度大，系统性、整体性、协同性很强。应对复杂的网络安全态势，必须做到统一谋划、统一部署、统一标准、统一推进。**要不断完善网络执法协作机制，尽快健全适应网络特点的规范化执法体系。**要落实网络安全法相关规定，加强网络安全执法队伍和执法能力建设，强化网信部门的统筹协调职责，明确各职能部门的权责界限和接口，形成网信、工信、公安、保密等各部门协调联动机制，既要防止职能交叉、多头管理，又要避免执法推责、管理空白，不断提高执法效率，有效维护网络空间的安全。考虑到互联网跨区域性强、地域边界不明显的特点，**要健全完善网络安全异地执法协作机制，实现区域之间执法联动。**还要破除部门利益，打通数据和信息壁垒，减少重复建设，**建立共享数据平台，切实做到不同部门收集的数据能够共享**，提高网络安全防范能力。

**（七）加快网络安全人才队伍建设**

　　网络安全是技术更新最快的领域之一，网络空间的竞争，归根到底是人才的竞争；建设网络强国，最关键的资源是人才。要高度重视网络安全人才培养工作，不仅要培养精通信息系统使用和维护的技术人才，还要培养大批能够开展网络安全风险监控、应急处置和综合防护的人才，从而满足网络安全法实施提出的要求。**要进一步加强网络安全学科建设**，优化师资队伍结构，改革人才培养模式，培养更多满足实践需要的应用型人才。要鼓励网络和信息化人才发展体制机制改革先行先试，**研究建立网络安全特殊人才培养、管理和激励制度**，加大对网络安全高端人才、紧缺人才的培养、引进和支持力度，使党政机关、关键信息基础设施运营单位能够**招得进、用得好、留得住**精通网络安全技术的“高、精、尖”专业人才。

　　当前，互联网已深度融入经济发展和社会生活的方方面面，深刻改变着人们的生产和生活方式。我们要认真学习、全面贯彻党的十九大精神特别是习近平新时代中国特色社会主义思想，进一步提高政治站位，牢固树立正确的网络安全观，进一步增强贯彻实施法律的紧迫感和自觉性，推进“一法一决定”各项制度全面落实，切实维护网络空间主权和人民群众切身利益，为决胜全面建成小康社会、夺取新时代中国特色社会主义伟大胜利、实现中华民族伟大复兴的中国梦提供坚强保障。