

中国网络空间安全法律与政策发展研究^{*}

张 衡^{**}

摘 要： 网络空间安全管理的制度化和法制化是全面推进依法治国的必然选择，是国家治理体系和治理能力现代化的题中应有之义。本报告梳理了近年来主要的网络空间安全立法、执法与政策措施，以“国家网络空间安全战略规划”为引领，重点关注“互联网信息传播治理”“计算机与网络犯罪”“个人信息保护”“诚信网络环境建设”“关键性基础设施安全保障”“移动互联网治理”等重要和前沿性领域的立法和执法的发展趋势，意在勾勒我国网络空间安全法律与政策的完整图景。

关键词： 网络空间安全 依法治国 网络治理

^{*} 本文为国家社科基金青年项目“大数据时代个人信息安全规制研究”（项目编号：14CTQ043）的阶段性研究成果。

^{**} 张衡，华东政法大学宪法学与行政法学博士研究生，上海社会科学院信息研究所助理研究员，主要从事数据保护与网络安全法律问题研究。



伴随着新技术、新应用的快速演进和发展，互联网在全球范围内掀起了一场影响人类各个层面的深刻变革，网络空间成为一种史无前例的信息沟通平台和互动场所。与此同时，正如乌尔里希·贝克在其“风险社会”理论中提出的“科学被普遍化的同时也被神秘化了，技术理性的扩张之下风险生产日益取代财富生产”，互联网与信息技术的运用也为国家安全、公共安全和个人安全带来了全新的风险。网络攻击、信息窃取、网络谣传、隐私侵害、病毒传播、网络犯罪、网络恐怖主义、网络监控等问题凸显网络空间存在的巨大风险和治理难题。加强和确保网络空间安全已经成为世界各国增强综合实力、保障国家安全的主要抓手。就中国而言，如何使拥有 6.49 亿网民^①的网络大国成为网络强国，如何在保持互联网开放性和创新性的同时预防和控制风险性和不确定性，如何不断提升互联网治理能力以积极参与全球互联网治理，这些问题都考验着决策者和管理者的智慧和决心。

面对日趋复杂和严峻的国际国内网络安全形势，党的十八届三中全会提出了“加大依法管理网络力度，加快完善互联网管理领导体制，确保国家网络和信息安全”的要求，网络空间安全的立法进一步加速。2014 年 2 月，习近平总书记在中央网络安全和信息化领导小组第一次会议上指出：“要抓紧制定立法规划，完善互联网信息内容管理、关键信息基础设施保护等法律法规，依法治理网络空间，维护公民合法权益。”党的十八届四中全会通过了《中共中央关于全面推进依法治国若干重大问题的决定》，这是新时期指导全面推进依法治国、加快建设法治中国的纲领性文件。^② 加强网络立法、网络执法、全网守法，进一步推进我国网络空间安全管理的制度化和法制化，设计既能确保网络空间安全、又能适应互联网发展需要的制度体系，也是国家治理体系和治理能力现代化的题中应有之义。

近年来，我国网络空间安全领域的立法活动十分活跃，以《全国人大常委会关于维护互联网安全的决定》《全国人大常委会关于加强网络信息保护的決定》《互联网信息服务管理办法》等法律法规为基础，制定颁布了一系列网

① 根据中国互联网信息中心（CNNIC）发布的第 35 次《中国互联网络发展状况统计报告》，截至 2014 年 12 月，我国网民规模达 6.49 亿。

② 鲁炜：《推进网络空间法治化》，新华网，http://news.xinhuanet.com/politics/2014-10/25/c_127139206.htm。

络安全管理的行政法规和部门规章。这一系列立法活动逐渐构建起中国网络空间安全的制度框架。本报告将梳理近年来主要的网络空间安全立法、执法与政策措施，以“国家网络空间安全战略规划”为引领，重点关注“互联网信息传播治理”“计算机与网络犯罪”“个人信息保护”“诚信网络环境建设”“关键性基础设施安全保障”“移动互联网治理”等重要和前沿性领域的立法和执法的发展趋势，试图勾勒我国网络空间安全法律与政策的完整图景。

一 中国网络空间安全的战略构想

中国自接入国际互联网以来 20 年间，制定和颁布了一系列具有战略意义的网络安全和信息化政策文件，信息网络安全也从“系统安全”“数据安全”逐步向“网络空间安全”演进。尤其是 2013 年以来，我国采取了一系列重大举措来加大网络安全和信息化发展的力度，从而确立了网络空间安全的战略地位。

（一）网络空间安全上升为国家战略

早在 2003 年，中共中央办公厅和国务院办公厅就发布了《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发〔2003〕27 号），简称《27 号文》，该文件首次将信息安全提升至促进经济发展、维护社会稳定、保障国家安全、加强精神文明建设的高度，从国家层面提出了“积极防御、综合防范”的信息安全管理方针，这是中国信息安全领域一次重要的战略部署，标志着中国网络信息安全保障进入了一个全新的阶段。2006 年，两办又发布了《2006—2020 年国家信息化发展战略》（中办发〔2006〕11 号），简称《11 号文》，这是中国信息化发展史上首次制定的中长期战略性发展规划，将信息化发展与信息安全保障相互融合，其中对建设国家信息安全保障体系和增强国家信息安全保障能力等方面进行了系统论述和政策安排。《11 号文》与《27 号文》一起成为中国网络信息安全战略的重要文件。2012 年，在中国信息化发展面临关键突破和信息安全面临严峻挑战的宏观背景下，国务院发布了《关于大力推进信息化发展和切实保障信息安全的若干意见》，将中国信息化发展与信息安全有机统一，在保障工业控制系统安全、强化信息资源和个人信



息保护及三网融合、云计算、物联网等领域安全技术和标准等方面做出具有针对性和前瞻性的政策安排，对健全中国信息安全保障体系、切实增强中国信息安全保障能力具有指导意义。^①

2014年2月27日，中央网络安全和信息化领导小组正式成立，这是党的十八届三中全会以后第三个由习近平任组长的跨党政军的重要机构。会上审议通过了《中央网络安全和信息化领导小组工作规则》《中央网络安全和信息化领导小组办公室工作细则》《中央网络安全和信息化领导小组2014年重点工作》等重要文件。在小组成立后的第一次会议上，习近平总书记做了“没有网络安全就没有国家安全”“没有信息化就没有现代化”“中国要建设网络强国”等重要指示。^②总书记的讲话体现了中国最高层保障网络安全、维护国家利益、推动信息化发展的决心，也肯定了网络空间安全在国家安全中的战略地位。

（二）网络信息安全的内涵与外延不断深化与拓展

近年来，互联网在“阿拉伯之春”“乌克兰危机”中扮演了重要角色，突发的政治更迭因为网络的助推而变得异常快速，境外敌对势力也将互联网作为对我国渗透破坏的主渠道^③；同时，网络谣言、网络色情、网络暴恐等有害信息在互联网上快速传播；网络恐怖主义、网络分裂主义通过互联网造谣生事，煽动暴恐活动，试图破坏我国社会稳定和国家安全；病毒传播、黑客入侵、信息滥用、网络欺诈等也造成了社会经济生活的重大损失。美国和以色列通过“震网”病毒攻击伊朗核设施，使关键基础设施的安全成为国家网络安全的核心内容。“棱镜门”事件则暴露美国正大规模监控各国政治、经济、军事、企业和个人秘密和敏感数据，凸显网络斗争日趋严峻和白热化。

信息化、网络化对经济、政治、社会等各领域的渗透和融合加剧了我国面临的国际、国内网络安全风险与挑战，信息网络安全的内涵与外延也在不断地

① 《信息安全辞典》，上海辞书出版社，2013，第120～124页。

② 《中央网络和信息化领导小组成立》，新华网，http://news.xinhuanet.com/info/2014-02/28/c_133148759.htm。

③ 《网络安全是重大战略问题——访国家互联网信息办公室副主任王秀军》，人民网，<http://www.people.com.cn/n/2014/0518/c348427-25031501.html>。

深化与拓展。网络空间安全面临着风险难以预期、参与主体众多、安全维护艰难复杂等困境。网络安全已经从传统的技术领域拓展为以政治安全为根本,包含意识形态安全、数据安全、技术安全、应用安全、资本安全和渠道安全等内容的总体安全的重要组成部分^①。同时,网络安全不仅仅涉及国家之间的合作与竞争,还包括国家与非国家行为体甚至个人之间的合作与竞争。

(三) 国家网络空间管理领导体制逐步完善和提升

自 20 世纪 80 年代起,我国开始建立信息化管理体制,也经历了一系列发展和演变。1996 年,在原国家经济信息化联席会议基础上成立了“国务院信息化工作领导小组”,统领全国信息化工作。^② 1999 年,国务院成立了“国家信息化工作领导小组”,不单设办事机构,具体工作由信息产业部承担。2001 年,中央决定重新组建“国家信息化领导小组”,组长由时任国务院总理朱镕基担任,同时成立国务院信息化办公室。2003 年,为了应对日益严峻的网络与信息形势,在国家信息化领导小组之下成立了国家网络与信息安全工作协调小组,组长由中央政治局常委、国务院副总理担任。2008 年国务院机构改革之后,国家信息化管理体制发生了较大的变化,国务院信息化办公室的工作职责划归新设的工业和信息化部,^③ 工业和信息化部负责协调维护国家信息安全和国家信息安全保障体系建设。2009 年,新一届国家网络与信息安全工作协调小组在国家信息化领导小组的领导下统筹协调跨部门的网络与信息安全工作,健全完善网络与信息安全工作部门间协同配合机制,协调处理网络与信息安全的重大事件。成员单位包括中办、国办、工信部、公安部、安全部等 17 个部门。2010 年工业和信息化部信息安全协调司加挂国家网络与信息安全工作协调小组办公室的牌子。2011 年国务院办公厅印发国家网络与信息安全工作协调小组工作规则,具体规定了协调小组职责、会议制度、通报制度,并进一步明确

① 《网络安全是重大战略问题——访国家互联网信息办公室副主任王秀军》,人民网, <http://politics.people.com.cn/n/2014/0518/c1001-25030371.html>, 访问时间:2014 年 9 月 10 日。

② 汪玉凯:《中央网络安全与信息化领导小组的由来及其影响》,人民网, <http://www.itgov.org.cn/Item/4167.aspx>, 访问时间:2014 年 9 月 10 日。

③ 汪玉凯:《中央网络安全与信息化领导小组的由来及其影响》,人民网, <http://www.itgov.org.cn/Item/4167.aspx>, 访问时间:2014 年 9 月 10 日。



了协调领导小组办公室各项具体职责——督促成员单位及相关部门贯彻落实协调小组的各项决定，研究网络与信息安全有关问题及动态，及时提出对策建议。

2014年成立的“中央网络安全和信息化领导小组”相比过去的“国家信息化工作领导小组”规格更高、立意更远，不仅仅是党中央层面设置的议事协调机构，也是最高决策机构，目的是为建设网络强国服务，为国家信息化全局战略服务。在网络空间安全日益成为全球竞争新焦点的背景下，以往的网络安全协调机制已经无法适应新时期的需要，只有进行集中统一领导，在组织架构上进行统筹协调，在重大复杂问题上进行战略决策，才能避免战略失误导致颠覆性错误的发生^①。该领导小组由习近平总书记担任组长，从总体上协调党委、军委、人大等机关，彻底改变长期以来我国网络安全管理存在的“九龙治水”乱局。同时，中央还成立了领导小组办公室，作为领导小组决定事项的落实机构。在地方层面，截至2014年8月底，共有河北、陕西、福建、吉林、四川、江苏、河南、贵州、河北、山东、甘肃、江西、广西、宁夏、北京等15个省（市、区）成立了由党委一把手担任组长的网络安全和信息化领导小组。在行政层面，2014年8月，国务院授权重新组建的国家互联网信息办公室负责互联网信息内容管理与监督执法，明确了互联网信息内容安全的监管主体。

（四）中国积极推进国际网络空间新秩序进程

1. 以“信息主权”为根本，提出中国版网络安全观

随着“棱镜门”事件的曝光和持续发酵，网络空间“信息主权”的争夺更趋激烈。网络空间的“信息主权”主要体现为对本国公民信息的控制权以及对跨境流动数据的管辖权上。2014年3月，巴西国会众议院表决通过《互联网民法》草案^②，明确要求跨国互联网公司做出承诺，在国外存储巴西公民信息时应遵守巴西相关法律，以防这些信息被窃。2014年4月，美国纽约南

① 汪玉凯：《中央网络安全和信息化领导小组的由来及其影响》，人民网，<http://www.itgov.org.cn/Item/4167.aspx>，访问时间：2014年9月10日。

② 《巴西国会众议院通过〈互联网民法〉草案》，人民网，<http://world.people.com.cn/n/2014/0326/c1002-24739287.html>，访问日期：2014年9月10日。

区法庭法官命令微软公司交出储存在该公司爱尔兰服务器内的资料,^①即认为美国对网络数据的管辖权不仅仅限于主权境内,还延伸到他国境内;与此同时,欧盟正通过修订《个人数据保护指令》做出规定,未来除非欧盟法律有明确规定或者是按照某个国际条约,不然企业不能将欧盟公民的资料交给其他国家。2014年7月,俄罗斯议会通过立法,要求从2016年起所有互联网公司必须将俄罗斯公民的数据转移到俄罗斯境内服务器上。^②德国与法国也在探讨建立欧洲独立互联网,拟从战略层面绕开美国以强化数据安全。^③

2014年7月16日,习近平主席在巴西国会发表的演讲中专门提到,“信息主权”不受侵犯,各国共同构建多边、民主、透明的国际互联网治理体系。根据公开报道,这一倡议是中国最高领导人首次在国际场合提出中国对互联网治理的主张。习近平在讲话中指出,“虽然互联网具有高度全球化的特征,但每个国家在信息领域的主权权益都不应受到侵犯,互联网技术再发展也不能侵犯他国的信息主权。在信息领域没有双重标准,各国都有权维护自己的信息安全,不能一个国家安全而其他国家不安全,一部分国家安全而另一部分国家不安全,更不能牺牲别国安全谋求自身所谓的绝对安全。国际社会要本着互相尊重和互相信任的原则,通过积极有效的国际合作,共同构建和平、安全、开放、合作的网络空间;建立多边、民主、透明的国际互联网治理体系”。^④

2. 多边合作,积极参与推进国际网络空间新秩序进程

自“棱镜门”事件以来,国际社会对制定相关国际规则、加强网络安全国际合作、规范网络空间行为的呼声日益高涨。巴西和德国呼吁将联合国《公民权利和政治权利国际公约》中有关保障隐私权的适用范围扩大到网络空间,两国共同提出了“数字时代的隐私权”决议草案,在2013年12月19日

① 《巴西国会众议院通过〈互联网民法〉草案》,人民网, <http://world.people.com.cn/n/2014/0326/c1002-24739287.html>, 访问日期:2014年9月10日。

② 《俄罗斯发互联网新规 俄公民数据必须存在国内服务器上》,路透社, <http://cn.reuters.com/article/CNTopGenNews/idCNKBSOFC08520140707>, 访问时间:2014年9月12日。

③ 《中央网络安全和信息化领导小组成立》,新华网, http://news.xinhuanet.com/info/2014-02/28/c_133148759.htm。

④ 习近平:《弘扬传统友好 共谱合作新篇——在巴西国会的演讲》,新华网, http://news.xinhuanet.com/2014-07/18/c_133492473_2.htm, 访问时间:2014年9月12日。



的联合国大会上得到通过;^① 印度表示愿意与巴西分享网络安全技术,以帮助巴西应对美国及其盟国进行的间谍监控;印度、巴西和南非三国还建议在联合国框架内建立一个新的机构来监督全球互联网治理。^②

我国要参与国际网络空间竞争,推进国家网络安全战略,就必须加强与国际社会的合作,在承认“网络信息主权”的基础上,发挥联合国等国际机构的作用,推动建立一个各国广泛参与、公正合理的互联网国际合作治理机制。早在2011年,我国就和俄罗斯、塔吉克斯坦、乌兹别克斯坦等国共同向联合国大会提交《信息安全国际行为准则》,并呼吁各国在联合国框架内就此展开进一步讨论,以尽早就规范各国在信息和网络空间行为的国际准则和规范达成共识。^③ 这份文件就维护信息和网络安全提出了一系列基本原则,涵盖政治、军事、经济、社会、文化、技术等各方面,包括各国不应利用包括网络在内的信息通信技术实施敌对行为、侵略行径和制造对国际和平与安全的威胁;各国有责任 and 权利保护本国信息和网络空间及关键信息和网络基础设施免受威胁、干扰和攻击破坏;建立多边、透明和民主的互联网国际管理机制;充分尊重在遵守各国法律前提下信息和网络空间的权利和自由;帮助发展中国家发展信息和网络技术;合作打击网络犯罪等。^④ 2014年6月23日召开的互联网名称与数字地址分配机构(ICANN)大会上,以美国准备放弃对ICANN的管理权为契机,国家互联网信息办公室主任鲁炜提出了互联网迈向全球共治时代的“七点共识”,倡议通过建立彼此互信,达成全球统一的行为准则。^⑤ 此外,以联合国安理会通过的打击“伊拉克-黎凡特伊斯兰国”和“支持阵线”等恐怖组织的决议(第2129号决议)为契机,我国还提出与国际社会就打击网络

① 《2013年国际十大信息安全热点事件》,人民网, <http://theory.people.com.cn/n/2014/0807/c387081-25421482.htm>, 访问时间:2014年9月12日。

② 《后“棱镜门”时代的网络安全:“去美国化”渐成气候》,王孔祥, http://theory.gmw.cn/2014-06/11/content_11582028.htm, 访问时间:2014年9月12日。

③ 《中俄等国向联合国提交“信息安全国际行为准则”文件》,新华网, http://news.xinhuanet.com/world/2011-09/13/c_122022390.htm。

④ 《中俄等国向联合国提交“信息安全国际行为准则”文件》,新华网, http://news.xinhuanet.com/world/2011-09/13/c_122022390.htm。

⑤ 《鲁炜呼吁国际网络空间治理形成七点共识》,新华网, http://news.xinhuanet.com/info/2014-06/24/c_133431878.htm, 访问时间:2014年9月12日。

恐怖主义加强合作，共同打击“东伊运”等恐怖势力的网络恐怖主义活动。^①2014年9月18日，在首届中国－东盟网络空间安全论坛上，中央网络安全和信息化领导小组办公室主任鲁炜在开幕式上提出，中国与东盟要加强互联互通，深化网络空间合作，并提出了中国网络空间理念：网络空间既要互联互通，也要尊重主权；既要加快发展，也要确保安全；既要提倡自由，也要遵守秩序；既要自主自立，也要开放合作。^②

二 中国互联网信息传播治理

信息自由传播是互联网的核心精神，但互联网自由并非没有边界，自由应该是在既有的法律制度框架内享有的，不侵犯他人合法权益的情况下行使权利。我国《宪法》第五十一条规定：“中华人民共和国公民在行使自由和权利的时候，不得损害国家的、社会的、集体的利益和其他公民的合法的自由和权利。”一旦个人的言论侵害了他人权益，政府就有义务制止这种行为，维护社会的正常公共秩序。这种秩序恰恰是全体公民正当的权利保障。网络无法脱离法律和制度的约束，对互联网信息传播进行规范是各国的通行做法。如何在控制有害信息传播的同时，保持互联网作为信息自由流动载体的优势，这也是各国面临的共同难题。

（一）中国互联网信息传播治理的主要做法

1. 构建民事、行政和刑事责任承担体系

我国互联网信息传播治理主要适用《刑法》《全国人大常委会关于维护互联网安全的决定》《互联网信息服务管理办法》《互联网新闻信息服务管理规定》等法律法规，对利用互联网以造谣等方式煽动颠覆国家政权、散布谣言扰乱社会秩序、侮辱或者诽谤他人、编造恐怖信息等行为均做出了明确规定。互联网用户，包括网民和网络内容提供商、服务提供商，须在法律允许范围内行事，侵害他人的合法权益要承担相应的民事、行政以及刑事责任。2000

① 《中方吁国际共同打击“东伊运”等网络恐怖主义活动》，中国新闻网，<http://www.chinanews.com/gn/2013/12-18/5635933.shtml>，访问时间：2014年9月12日。

② 《鲁炜：“打造中国－东盟信息港，携手构建网络空间共同体”》，新华网，http://www.gx.xinhuanet.com/topic/20104dm/2014-09/18/c_1112539105.htm。



年,《全国人大常委会关于维护互联网安全的决定》规定了与互联网信息传播相关的六类犯罪行为。《互联网信息服务管理办法》则进一步明确了互联网信息服务提供者不得制作、复制、发布、传播的内容信息。此外,2001年通过的《刑法修正案(三)》还增加了编造、故意传播虚假恐怖信息罪的罪名;而对于言论自由相对于其他公民权利的限制,《刑法》在分则部分规定了侮辱罪、诽谤罪、诬告陷害罪、煽动民族仇恨罪、民族歧视罪等罪名。^①

2. 推行以“用户实名”为基础的互联网治理方式

2011年12月,北京市公布《北京市微博客发展管理若干规定》(以下简称《规定》),提出任何组织或个人注册微博客账号应当使用真实身份信息;网站开展微博客服务应当保证注册用户信息真实。《规定》率先提出了微博实名制的要求。2012年全国人大常委会通过《关于加强网络信息保护的决定》(以下简称《决定》),正式将“网络实名制”上升至法律层面,规定了“网络服务提供者为用户办理网站接入服务,办理固定电话、移动电话等接入互联网手续,或者为用户提供信息发布服务,应当在与用户签订协议时,要求用户提供真实身份信息”。这意味着用户在使用微博、博客、BBS等提供信息发布的互联网服务时必须实名注册。2013年3月,国务院办公厅《关于实施〈国务院机构改革和职能转变方案〉任务分工的通知》将出台并实施信息网络实名登记制度列为2014年的工作任务。2013年7月,根据《决定》和《国务院机构改革和职能转变方案》的要求,为了治理电话传播淫秽电子信息、垃圾短信、有害信息、短信网络诈骗等危害用户合法权益,扰乱社会秩序,甚至威胁国家安全的行为,工信部发布了《电话用户真实身份信息登记规定》(以下简称《规定》),明确用户真实身份信息登记的范围、程序、要求和信息保护等制度。《规定》第三条规定,“电信业务经营者为用户办理固定电话、移动电话(含无线上网卡)等入网手续,在与用户签订协议或者确认提供服务时,如实登记用户提供的真实身份信息。”

3. 加大平台责任,构建多主体共治治理范式

自2007年中办《关于加强网络文化建设和管理的意见》(中办发〔2007〕16号)中提出“谁经营谁负责、谁办网谁负责”的要求后,加大网络平台责

^① 高铭喧、张杰:《宪法权利的刑法保护——以言论自由为例的解读》,《湘潭大学学报》(哲学社会科学版)2006年第6期。

任就成为我国立法的明显趋势。《全国人大常委会关于加强网络信息保护的決定》第五条规定了互联网服务提供者信息发布和传输的监管责任：“网络服务提供者应当加强对其用户发布的信息的管理，发现法律、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，保存有关记录，并向有关主管部门报告。”同时，第十条规定“有关主管部门依法履行职责时，网络服务提供者应当予以配合，提供技术支持”，强调互联网服务提供者在主管部门履职时应予以配合的责任。2014年8月，国家互联网信息办公室发布的《即时通信工具公众信息服务发展管理暂行规定》第五条也规定了即时通信工具服务提供者的平台责任，要求即时通信工具服务提供者落实安全管理责任，建立健全各项制度，配备与服务规模相适应的专业人员，保护用户信息及公民个人隐私，自觉接受社会监督，及时处理公众举报的违法和不良信息。此外，平台方也积极推动行业自律，比如2012年新浪微博与用户共同制定《新浪微博社区公约》，以行业自律的方式推动网络谣言治理。

值得注意的是，立法需要进一步明确“法律、法规禁止发布或者传输的信息”的范围，强调禁止发布或传输信息的范围只能由法律法规规定；防止网络服务提供者超越法律法规的授权权限，阻碍互联网用户正常使用网络服务；为互联网用户提供维护权利的救济渠道。此外，互联网治理也必须符合必要性原则和比例原则，通过合理确定互联网服务提供者的责任范围，避免过度增加平台方的负担，增加企业运营成本，影响互联网企业的服务与创新。

4. 以“审查许可”模式规范互联网信息服务提供商的资质

我国对经营性互联网服务实行“审查许可制”，其依据是2000年国务院制定的《互联网信息服务管理办法》（以下简称《办法》）。根据该《办法》第四条的规定，“国家对经营性互联网信息服务实行许可制度；对非经营性互联网信息服务实行备案制度。未取得许可或者未履行备案手续的，不得从事互联网信息服务。”《办法》第十一条规定“互联网信息服务提供者应当按照经许可或者备案的项目提供服务，不得超出经许可或者备案的项目提供服务”。此外，互联网服务提供商还必须保证所提供的信息内容合法。我国的审查许可模式要求互联网提供商在取得政府许可之后才能进行互联网服务，否则将会面临网站关闭、罚款等行政处罚。互联网信息服务提供商的信息服务必须合法，否则将会受到吊销许可证的处罚。针对微信等新兴即时通信工具，国家互联网信息办公室2014年8



月发布了《即时通信工具公众信息服务发展管理暂行规定》(以下简称《暂行规定》)。根据该《暂行规定》,即时通信工具服务提供者应当具备互联网新闻信息服务资质。只有新闻单位、新闻网站开设的公众账号才可以发布、转载时政类新闻;取得互联网新闻信息服务资质的非新闻单位开设的公众账号可以转载时政类新闻。国家新闻出版广电总局《关于进一步完善网络剧、微电影等网络视听节目管理的补充通知》也要求,“从事生产制作网络剧、微电影等网络视听节目的机构,应依法取得广播影视行政部门颁发的‘广播电视节目制作经营许可证’。互联网视听节目服务单位不得播出未取得‘广播电视节目制作经营许可证’机构制作的网络剧、微电影等网络视听节目。”

(二) 开展净网行动,使“网络空间晴朗起来”

自2013年8月19日习近平总书记在全国宣传思想工作会议上提出“要使网络空间晴朗起来”的要求以来,全国范围内开展了一系列以“营造晴朗网络空间”为主旨的专项行动,集中打击网络谣言、网络色情信息、网络恐怖信息的传播,规范网络管理,净化网络环境。

1. 打击网络谣言

互联网具有的公共性、匿名性、便捷性等特点,使其成为新的犯罪平台。从2013年5月起,国家互联网信息办开始在全国范围内集中部署打击利用互联网造谣和故意传播谣言的行为。^①2013年9月9日,最高人民法院、最高人民检察院发布《最高人民法院、最高人民检察院关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释》(以下简称《解释》),为网络言行划定法律边界。《解释》对利用信息网络“捏造事实诽谤他人”及实施诽谤行为“情节严重”的认定,对利用信息网络实施诽谤犯罪适用公诉程序的条件以及利用信息网络实施寻衅滋事、敲诈勒索、非法经营等犯罪的认定,打击信息网络共同犯罪等8方面的问题进行了明确规定,^②对规范网络管理、净化

① 《国家互联网信息办部署打击网络谣言》,新华网, http://news.xinhuanet.com/politics/2013-05/02/c_115612608.htm, 访问时间:2014年9月12日。

② 《最高人民法院、最高人民检察院发布〈关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释〉》,中国法院网, <http://www.chinacourt.org/article/detail/2013/09/id/1081084.shtml>。

网络环境起到了积极的推动作用。根据《解释》，同一诽谤信息实际被点击、浏览次数达到五千次以上，或者被转发次数达到五百次以上的，应当认定为刑法第二百四十六条第一款规定的“情节严重”。

2. 打击网络淫秽色情信息

2014年4月始，“扫黄打非”工作小组办公室、国家互联网信息办公室、工业和信息化部、公安部联合发布了《关于开展打击网上淫秽色情信息专项行动的公告》，宣布在全国范围内统一开展打击网上淫秽色情信息“扫黄打非·净网2014”专项行动。^①该行动主要依据《刑法》和《最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》等法律与司法解释，对制作、复制、出版、贩卖、传播淫秽电子信息涉嫌构成犯罪的，依法追究刑事责任；对为淫秽色情信息传播提供条件的电信运营服务、网络接入服务、广告服务、代收费服务等经营者，依法追究相关刑事责任。对互联网企业提出自查自纠，主动清理网上淫秽色情信息或链接，严格落实信息安全管理制，完善内容审核把关机制，研发应用防范淫秽色情信息传播的技术措施等责任要求。^②根据国家互联网信息办公室的通报，截至2014年6月20日，自“净网”专项行动开展以来，已累计处理、关闭淫秽色情网站1222家。被查处的淫秽色情网站主要有四类：一是传播色情影片的无资质视频类网站，二是发布淫秽色情内容的图片类网站，三是散布色情信息的医疗健康类网站，四是境内空壳类网站链接境外色情网站。^③在此次行动中，国内著名门户网站新浪网因传播淫秽色情信息而被吊销“互联网出版许可证”和“信息网络传播视听节目许可证”，并处以5至10倍于违法金额的罚款；^④国内颇具影响的视频网站快播因通过互联网传播淫秽色情信息，情节严重，遭到吊销增值

① 《关于开展打击网上淫秽色情信息专项行动的公告》，新华网，http://news.xinhuanet.com/legal/2014-04/13/c_1110219590.htm。

② 《关于开展打击网上淫秽色情信息专项行动的公告》，新华网，http://news.xinhuanet.com/legal/2014-04/13/c_1110219590.htm。

③ 《“净网”专项行动关闭色情网站1222家》，新华网，http://news.xinhuanet.com/2014-06/20/c_1111247082.htm。

④ 《新浪涉嫌传播淫秽色情信息被吊销互联网出版许可证等》，新华网，http://news.xinhuanet.com/newmedia/2014-04/25/c_126433003.htm。



电信业务经营许可证的行政处罚。^①

3. 打击虚假恐怖信息

针对网络上种种编造、故意传播虚假恐怖信息，严重影响社会稳定、扰乱社会公共秩序的违法行为，2013年，最高院对外公布了《最高人民法院关于审理编造、故意传播虚假恐怖信息刑事案件适用法律若干问题的解释》（以下简称《解释》）。《解释》对“虚假恐怖信息”做了明确的定义，是指“以发生爆炸威胁、生化威胁、放射威胁、劫持航空器威胁、重大灾情、重大疫情等严重威胁公共安全的事件为内容，可能引起社会恐慌或者公共安全危机的不真实信息”。《解释》规定了量刑的三个档次：一个是入罪的档次，一个是从重处罚的档次，一个是五年以上判处刑法的档次。多次编造故意传播虚假恐怖信息达三次以上，应当在五年以下有期徒刑范围内酌情从重处罚。

4. 打击暴恐影音传播

针对“东突”等分裂势力在境外网站发布危害极大的暴力恐怖、极端宗教思想的音视频信息，国家互联网信息办公室2014年6月启动了“铲除网上暴恐音视频”专项行动，包括坚决封堵境外暴恐音视频，在全国全网集中清理网上暴恐音视频，查处一批违法网站和人员，落实企业管理责任，畅通民间举报渠道等。2014年9月，最高人民法院、最高人民检察院与公安部联合出台《关于办理暴力恐怖和宗教极端刑事案件适用法律若干问题的解释》（以下简称《意见》）。《意见》规定，除散布暴恐音视频者外，允许或放任他人散布音视频的相关人员，也要以共同犯罪论处。

5. 规范即时通信工具公众信息服务

随着移动互联网时代的到来，以微信为代表的即时通信工具成为应用最广泛的互联网服务之一。^②与此同时，许多涉恐、涉暴、涉黄等违法信息以及诽谤和谣言信息也借助即时通信工具用户规模巨大、信息传播迅速、用户间信任度高等特点被广泛传播，严重扰乱社会秩序和社会稳定。2014年8月，国家互联网信息办公室出台《即时通信工具公众信息服务发展管理暂行规定》（以下简称《暂行规

① 《快播公司被吊销增值电信业务经营许可证》，新华网，http://news.xinhuanet.com/fortune/2014-06/28/c_1111363981.htm。

② 根据CNNIC《2014年中国社交类应用用户行为研究报告》的调查显示，即时通信在整体网民中的覆盖率为89.3%。

定》),使“即时通信工具公众信息内容”管理进入有法可依的时期,即时通信工具的生态环境得以净化。《暂行规定》从行业资质、隐私保护、实名注册、备案审核、内容限制等方面对即时通信平台及用户行为进行规范。一是明确了微信等即时通信工具服务提供商的平台责任,要求取得相关资质、落实安全管理责任、健全各项制度、配备相应人员,保护用户隐私,接受社会监督,及时处理举报信息;二是落实即时通信工具用户实名制,用户通过真实身份信息认证后注册账号,也即实行“实名注册”;三是明确微信公众号采用备案审查制度,对微信公众号等即时通信工具公众信息服务者开设公众账号,必须经过即时通信工具服务提供商审核,同时由即时通信工具服务提供商向互联网信息服务主管部门分类备案;四是严格限制时政类文章的发布和转载,要求公众号管理者必须具备相关资质,要求并规定除新闻单位、新闻网站、取得互联网新闻信息服务资质的非新闻单位开设的公众账号之外,其他公众账号未经批准不得发布、转载时政类新闻。根据2005年制定的《互联网新闻信息服务管理规定》,时政类新闻信息“包括有关政治、经济、军事、外交等社会公共事务的报道、评论,以及有关社会突发事件的报道、评论”。但平台方如何具体落实“时政类新闻”的界定有待进一步明确。

三 计算机与网络犯罪

2014年6月,美国战略与国际问题研究中心(CSIS)发表报告指出,网络犯罪每年给全球带来约4450亿美元的经济损失,并指出网络犯罪正处于增长期,对贸易、竞争和创新都造成了严重影响。^①根据2001年《网络犯罪公约》的规定,网络犯罪可以分为非法存取、非法截取、资料干扰、系统干扰、设备滥用、伪造资料、电脑诈骗、儿童色情、侵犯版权等9项网络犯罪行为。

截至2014年底,我国与计算机和网络犯罪有关的刑事立法主要包括《刑法》《全国人大常委会关于维护互联网安全的决定》《电信管理条例》《计算机信息系统安全保护条例》《计算机软件保护条例》《计算机病毒防治管理办法》《信息安全登记保护管理办法》《计算机信息网络国际联网管理暂行规定》,以

^① James Andrew Lewis, Stewart Baker, “The Economic Impact of Cybercrime and Cyber Espionage,” http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf.



及《最高人民法院、最高人民检察院、公安部关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》等法律法规和司法解释。

为集中遏制黑客地下产业链的蔓延发展，健全防治黑客地下产业链的长效机制，工业和信息化部 2013 年实施了“治理黑客地下产业链专项行动”，主要任务包括：落实《木马和僵尸网络监测与处置机制》，加强对木马和僵尸网络的监测和研判；加强对仿冒政府、金融、传媒、电子商务类网站的监测和研判；落实《移动互联网恶意程序监测与处置机制》，加强对移动互联网恶意程序网络监测，开展移动互联网应用程序安全检测等。^①

针对网络犯罪跨地域、虚拟性、隐蔽性的特点且涉案人员散布多地的特点，2014 年 7 月，《最高人民法院、最高人民检察院、公安部关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》发布（以下简称《意见》），对打击网络犯罪实践中迫切需要解决的案件管辖、证据收集等问题做出规定。^②《意见》将网络犯罪案件分为四类：危害计算机信息系统安全犯罪案件；通过危害计算机信息系统安全行为进而实施的盗窃、诈骗等其他犯罪案件；在计算机网络上设立主要用于实施犯罪活动的网站、通信群组或者发布信息，针对或者组织、教唆、帮助不特定多数人实施的犯罪案件；其他主要犯罪行为在网络上实施的案件。在犯罪地认定上，《意见》将“犯罪行为发生地的网站服务器所在地”的表述修正为“用于实施犯罪行为的网站服务器所在地”，从而避免了歧义。针对网络犯罪涉案人数众多且无法逐一收集相关言词证据的问题，《意见》指出，在慎重审查被告人的辩解及其辩护人的辩护意见及相关证据的基础上，可以综合全案证据，依据电子数据、书证等证据记录的情况，认定被害人数、被侵害的计算机信息系统数量、涉案资金数额等犯罪事实。

四 安全诚信的网络环境建设

2014 年 6 月，国务院印发《社会信用体系建设规划纲要（2014—2020

① 《工业和信息化部关于印发防范治理黑客地下产业链专项行动方案的通知》，工业和信息化部网站，<http://www.miit.gov.cn/n11293472/n11293832/n12843926/n13917072/15567197.html>。

② 《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》，公安部网站，<http://www.mps.gov.cn/n16/n1996048/n1996090/n1996180/4071756.html>。

年)》(以下简称《规划纲要》),意在加快建设社会信用体系,构筑诚实守信的经济社会环境。为了建设可信网络,《规划纲要》针对加强网上诚信建设提出了四个方面的措施:第一,逐步落实网络实名制,强化网民对自己在网上的言行负责的意识。第二,建立网络信用档案,涵盖互联网企业和网民的信用档案,并且要与社会其他领域相关信用信息进行交换共享,促进在社会各领域的推广应用。第三,建立网络信用评价体系,对互联网企业的服务经营行为、上网人员的网上行为进行信用评估,记录信用等级。第四,建立网络信用黑名单制度,将实施网络欺诈、造谣传谣、侵害他人合法权益等严重网络失信行为的企业、个人列入黑名单,对黑名单主体采取网上行为限制、行业禁入等措施,并通报相关部门进行公开曝光。此外,为了营造安全可信的信息消费环境,正在起草的《电子商务法》也将突出强调网购信用体系建设。国家工商行政管理总局起草的《网络商品交易及有关服务管理办法(征求意见稿)》也提出了网店实名制等要求建立网购信用体系。深圳出台的全国首个网络经营者信用管理办法《深圳市网络经营者交易信用信息管理办法》规定:“网络经营者交易信用信息提供者、信息主体因故意或重大过失向可信交易公共服务机构提供虚假或伪造的信息;或网络经营者交易信用信息使用人违法使用信息,侵犯企业合法权益或个人隐私,给当事人造成损失的,依法追究法律责任;涉嫌犯罪的,依法移交司法机关。”

五 保障个人信息安全

2011年以来,一系列恶性个人信息泄露事件(如中国软件开发联盟6000万个人信息被黑客公开、中国人寿80万客户保单信息泄露、2000万酒店住宿信息泄露)的发生凸显我国个人信息安全的脆弱现状。与此同时,大数据时代的数据资源正呈现爆发式、多样性的增长态势,并且由于数据聚合和挖掘技术的发展,对个人数据的收集和利用成为新应用新业态发展的基础内容,个人信息安全风险也变得更为严重。

2012年12月全国人大常委会第三十次会议通过的《关于加强网络信息保护的决定》(以下简称《决定》)成为我国个人信息保护的基础性法律。《决定》将“个人信息保护”从各部门法和部委规章中的零散规定首次提升到单



独的“法律”规范层面。《决定》规定了网络服务提供者和其他企事业单位在业务活动中收集、使用、保存公民个人信息的行为应当遵循的原则，简而言之，就是“规则明示公开、征得对方同意、确保信息安全”。2013年6月，工业和信息化部发布了《电信和互联网用户个人信息保护规定》，进一步明确了电信业务经营者、互联网信息服务提供者收集和使用用户个人信息的规则以及相关信息安全保障措施。2014年8月发布的《工业和信息化部关于加强电信和互联网行业网络安全工作的指导意见》中要求严格规范用户个人信息的收集、存储、使用和销毁等行为，落实各个环节的安全责任，完善相关管理制度和技术手段；落实数据安全和用户个人信息安全防护标准要求，完善网络数据和用户信息的防窃密、防篡改和数据备份等安全防护措施；强化对内部人员、合作伙伴的授权管理和审计，加大违规行为惩罚力度；发生大规模用户个人信息泄露事件后要立即向通信主管部门报告，并及时采取有效补救措施。

2013年10月，全国人大常委会修改了《消费者权益保护法》，将个人信息保护作为消费者的一种权益确认下来。新修改的《消费者权益保护法》规定了经营者收集、适用消费者个人信息应当遵循的原则，以及经营者及其工作人员的保密义务和安全保障责任。此外，人口健康信息作为重要的信息资源而与个人隐私密切相关，2014年5月，国家卫计委印发《人口健康信息管理办法（试行）》，提出医院泄露个人电子病历将被追责，规定责任单位采集、利用、管理人口健康信息应当遵循医学伦理原则，保护个人隐私，对违反规定泄露个人健康信息的，情节严重的可依法追究法律责任。

六 关键性基础设施安全保障

“棱镜门”事件与频频发生的“黑客攻击”等安全事件发生后，信息网络安全被提升至国家战略高度。其中，关键性基础设施安全保障成为网络空间安全的重要内容，我国也制定了一系列法律和政策措施来保障其安全。

（一）强化关键信息基础设施保护

2013年美国奥巴马颁布了《国家网络安全和关键基础设施保护法案》的政策指令，要求国土安全部明确政府各部门对“关键基础设施”安全的责



任,这对我国加强关键基础设施网络安全建设具有重要的借鉴意义。所谓“关键基础设施”部门,指的是那些至关重要的、实体的或虚拟的系统或资产,这些系统或资产遭到破坏或丧失功能将危及国家安全、国家经济安全、国家公共健康和社会稳定。根据《电信法》和《通信网络安全防护管理办法》,我国对通信网络的安全防护进行了规范,“防止通信网络阻塞、中断、瘫痪或者被非法控制,防止通信网络中传输、存储、处理的数据信息丢失、泄露或者被篡改”;^①并且要求“通信网络运行单位新建、改建、扩建通信网络工程项目,应当同步建设通信网络安全保障设施,并与主体工程同时进行验收和投入运行”。^②2011年,工信部《关于加强工业控制系统信息安全管理的通知》提出,对核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、铁路、城市轨道交通、民航、城市供水供气供热以及其他与国计民生紧密相关的领域,要加强信息安全检查、监管和测评,实施安全风险和漏洞通报制度。2013年,《国家发展改革委关于加强和完善国家电子政务工程建设管理的意见》对电子政务工程建设管理提出了“保障电子政务项目安全可控”的要求,包括“统一使用国家网络信任服务设施”“加强信息系统分级保护和等级保护”“积极采用安全可控信息技术和产品”;要按照《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》的要求开展信息安全风险评估,涉密信息系统投入使用前应该经保密行政管理部门审查批准。

(二) 提升突发网络安全事件应急响应能力

2009年,工业和信息化部颁布《公共互联网网络安全应急预案》,2014年,工信部又颁布《关于加强电信和互联网行业网络安全工作的指导意见》,对完善网络安全应急预案提出了一系列要求,包括健全大规模拒绝服务攻击、重要域名系统故障、大规模用户信息泄露等突发网络安全事件的应急协同配合机制;加强应急预案演练,定期评估和修订应急预案,确保应急预案的科学性、实用性、可操作性;提高突发网络安全事件监测预警能力,加强预警信息发布和预警处置,对可能造成全局性影响的要及时报通信主管部门;严格落实

^① 见工业和信息化部,《通信网络安全防护管理办法》第二条第三款。

^② 见工业和信息化部,《通信网络安全防护管理办法》第六条第一款。



突发网络安全事件报告制度；建设网络安全应急指挥调度系统，提高应急响应效率；根据有关部门的需求，做好重大活动和特殊时期对其他行业重要信息系统、政府网站和重点新闻网站等的网络安全支援保障。

（三）进一步推进信息安全产业扶持政策

我国尚未形成自主可控的计算机技术、软件技术和电路技术，重要信息系统、关键基础设施中使用的核心技术产品和关键服务还严重依赖国外，如何强化我国核心技术领域的研究能力，形成具有竞争力的信息安全产业链，是产业扶持政策的核心内容。

2013年，工信部《信息化和工业化深度融合专项行动计划（2013—2018年）》提出，“加快集成电路、关键电子元器件、基础软件、新型显示、云计算、物联网等核心技术创新，突破专项行动急需的应用电子、工业控制系统、工业软件、三维图形等关键技术；围绕工业重点行业应用形成重大信息系统产业链配套能力，开展国产中央处理器（CPU）与操作系统等关键软硬件适配技术联合攻关，提升产业链整体竞争力和安全可控发展能力；支持面向云计算、移动互联网、工业控制系统等关键领域安全技术研发与产业化，加快安全可靠通信设备、网络设备等终端产品研发与应用。”2013年8月，国家发改委公布《关于组织实施2013年国家信息安全专项有关事项的通知》，针对金融、云计算与大数据、信息系统保密管理等领域组织国家信息安全专项。根据专项，国家将支持金融信息安全领域、云计算与大数据信息安全领域、信息安全分级保护领域、工业控制信息安全领域的信息安全产品产业化。2014年6月，国务院发布《国家集成电路产业发展推进纲要》，成立国家集成电路产业发展领导小组，设立国家产业投资基金，加大财税支持力度，推动国产芯片产业的发展，以此摆脱我国对国外集成电路的依赖。^①

（四）以国产替代保障网络安全可管可控

“棱镜门”事件曝光之后，我国开始高度重视网络安全与自主可控的问

^① 《国务院印发〈国家集成电路产业发展推进纲要〉》，新华网，http://news.xinhuanet.com/2014-06/24/e_1111293998.htm。

题。据悉,有关部门正在着手准备调研并起草“信息安全装备国产化”专项扶持方案,重点调研服务器和路由器的国产化问题。^① 2014年5月16日,中央国家机关政府采购中心下发《关于进行信息类协议供货强制节能产品补充招标的通知》,其中规定,国家机关在“信息类协议供货强制节能产品采购招标”中,所有计算机类产品不允许安装 Windows 8 操作系统。这一行动掀开了国产化替代的序幕。2014年9月,银监会发布《关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见》明确提出,到2019年,安全可控信息技术在银行业总体达到75%的使用率,金融行业“去IOE”行动也正式启动。

(五) 探索建立国家网络安全审查制度

对信息技术产品及其供应商开展不同形式的网络安全审查是各国通行的做法。美国、英国等国在互联网基础设施建设过程中都建立了极为严格细致的网络安全审查制度,由多个安全部门共同参与审查,根据安全部门的标准进行施工。为应对应用日益广泛的云计算,美国政府还针对云计算服务提供者进行安全审查,并明确规定联邦政府部门只能选择通过审查的云计算服务提供者提供的服务。^② 2014年5月,工业和信息化部发布了《通信工程建设项目招标投标管理办法》,8月又发布了《关于加强电信和互联网行业网络安全工作的指导意见》。针对通信工程建设项目,在关键软硬件采购招标时要统筹考虑网络安全需要,在招标文件中明确对关键软硬件的网络安全要求。关键软硬件采购前要进行网络安全检测评估,通过合同明确供应商的网络安全责任和义务,要求供应商签署网络安全承诺书,初步提出了通信领域的网络安全审查要求。

七 移动互联网安全治理

(一) 恶意程序治理

根据中国互联网络信息中心(CNNIC)发布的《2013—2014年中国移动

① 《传国内酝酿信息安全装备国产化扶持政策》,凤凰网, http://finance.ifeng.com/a/20140612/12529305_0.shtml。

② 《我国将出台信息安全审查制度》,新华网, http://news.xinhuanet.com/politics/2014-05/22/c_1110810914.htm。



互联网调查研究报告》显示，截至 2014 年 6 月，我国手机网民规模为 5.27 亿，在整体网民中占比达 83.4%。移动互联网应用的丰富程度加大，以及对社会生活服务渗透增加，成为手机网民常态的生活方式和各行业的重要发展模式。移动互联网的迅速发展极大地促进了经济社会的发展和进步。但与此同时也出现了利用移动互联网进行恶意扣费、窃取信息、钓鱼欺诈等恶意程序，危害网络和信息安全，损害人民群众利益。

2013 年 11 月，工信部发布了《关于加强移动智能终端进网管理的通知》，对移动智能终端进网管理做出具体要求，要求手机厂商预装软件必须通过工业和信息化部审核，明令禁止五类应用软件：未向用户明示并经用户同意，擅自收集、修改用户个人信息的；擅自调用终端通信功能，造成流量消耗、费用损失、信息泄露等不良后果的；影响移动智能终端正常功能或通信网络安全运行的；含有《中华人民共和国电信条例》禁止发布、传播的信息内容的；其他侵害用户个人信息安全和合法权益以及危害网络与信息安全的。^① 2014 年 4 月开始，工信部、公安部和工商总局在全国范围内联合开展了打击移动互联网恶意程序的专项行动，印发了《打击治理移动互联网恶意程序专项行动工作方案》。^② 方案从预装应用程序管理、应用商店责任、应用程序开发者第三方签名认证、恶意程序监测处置等方面提出了具体的工作措施。未来，工信部还将研究制定移动互联网应用安全管理办法，探索建立移动应用程序第三方安全检测机制。^③

（二）垃圾短信治理

针对“伪基站”发送垃圾短信问题，工信部 2013 年 6 月发布《关于开展深入治理垃圾短信息专项行动的通知》，专项治理垃圾短信。^④ 根据工信部的

① 《工业和信息化部关于加强移动智能终端进网管理的通知》，工业和信息化部网站，http://www.gov.cn/jwqk/2013-10/31/content_2518541.htm。

② 《三部门开展打击治理移动互联网恶意程序专项行动》，中央政府门户网站，http://www.gov.cn/xinwen/2014-04/30/content_2669404.htm。

③ 《我国将制定移动互联网应用安全管理办法》，新华网，http://news.xinhuanet.com/2014-08/27/c_1112255176.htm。

④ 《工业和信息化部关于开展深入治理垃圾短信息专项行动的通知》，工业和信息化部网站，<http://www.miit.gov.cn/n11293472/n11293832/n11293907/n11368223/15351360.html>。

要求,基础电信企业必须建立全国范围内跨企业、跨地区的垃圾短信息治理协调支撑平台,并强化数据分析挖掘能力;切断垃圾短信利益链;重点清理基础电信企业自有及合作的端口类短信息发送业务。2014年11月4日,工业和信息化部又就《通信短信息服务管理规定(征求意见稿)》,向社会公开征求意见。意见稿规定,对违反“未经用户同意不得发送商业性短信”的基础电信业务经营者和短信息服务提供者,由电信管理机构责令限期改正,予以警告,可以并处一万元以上三万元以下罚款,向社会公告。^①此外,工信部还将研究制定《反垃圾信息框架技术要求》,推动落实《移动终端垃圾短消息过滤技术要求》等反垃圾信息技术标准。^②工信部还将联合最高法、法制办、公安部等相关部门推动修订《最高人民法院关于审理破坏公用电信设施刑事案件具体应用法律若干问题的解释》和《最高人民法院关于审理扰乱电信市场管理秩序案件具体应用法律若干问题的解释》,对利用“伪基站”破坏公用电信设施、扰乱电信市场管理秩序和无线电通信管理秩序的行为加大惩处力度。此外,工信部还将联合公安、工商等部门,对“伪基站”等违法违规电信设备的生产、销售、使用等产业链的各个环节开展集中整治专项行动,重点打击源头生产企业,遏制“伪基站”蔓延态势。^③

八 未来展望

(一) 确立“发展”“开放”“权利保护”的立法理念

在立法理念上,一是要厘清安全与发展的关系。一方面,我国传统信息安全立法思维管制色彩过浓,容易陷入“禁止+处罚”式的监管模式,阻碍新技术新应用的发展和公民基本权利的保障。另一方面,由于网络安全事关国家

① 《公开征求对〈通信短信息服务管理规定(征求意见稿)〉的意见》,工业和信息化部网站, <http://www.miit.gov.cn/n11293472/n11293832/n12845605/n13916913/16221817.html>。

② 《工信部出台法规整治垃圾短信,运营商从源头杜绝》,新华网, http://news.xinhuanet.com/info/2013-06/21/c_132473018.htm。

③ 《工信部将联合相关部门修法治理“垃圾短信”》,《中国日报》, http://www.chinadaily.com.cn/hqgj/jryw/2014-02-27/content_11298386.html。



重大战略利益，没有网络安全，就没有国家安全，互联网的发展也是无本之木，缺乏根基。在中央网络安全和信息小组成立之后召开的第一次全体会议上，习近平总书记适时提出了“网络安全与信息化是一体之两翼、驱动之双轮”的战略思想，为我国处理好安全与发展的关系指明了方向。安全与发展并非对立，没有发展就没有安全，安全应当融入发展的概念内涵之中。二是要厘清安全与开放的关系。自20世纪90年代以来，互联网的繁荣发展归功于其开放互联的本质特征。互联网的发展推动了信息的自由流动和开放共享，与此同时，世界各国对于数据资源的主权和管辖权的争夺也日趋激烈。如何在保障开放互联的基础上实现本国网络空间的战略利益，这是当今世界的一大难题。但必须明确的是，以网络空间安全和数据安全为名争夺数据主权，并不是要在互联网上根据国界建立起防火墙，割裂互联网，而是通过国家间的协商共治来使技术能力不同的国家拥有平等使用数据资源的权利。三是要厘清个人利益与国家利益之间的关系。在网络安全风险成为政府和社会关注的焦点后，政府常常以满足国家与公众的安全需求为由为自己赋权，造成政府公权力的扩张，相应缩限个人权利。为了维护安全而与个人或团体利益发生冲突的情况多有发生，比如网络监控与个人隐私保护、网络言论自由与网络信息过滤等。因此，公权力的行使必须要符合维护安全目的的必要性和比例原则，防止在公共利益的模糊概念之下藏着特定集团的利益或者滥用力量的现象。

（二）以“透明”、“共治”和“责任”为重点，构建多元合作的互联网治理模式

一是进一步增强政府透明度和开放度，以公开和透明应对网络谣言。要挤压谣言传播的空间，最有效的办法就是让政府信息公开制度真正有效运作起来。政府要对于公众普遍关心的重大和敏感问题及时通过各种渠道发布信息，让信息公开的速度快于谣言传播的速度，这样才能真正使谣言消失在“阳光”下，形成政府和社会公众共同参与的防范网络谣言的制度壁垒。二是推动多主体共同参与网络信息传播治理，明确各利益主体的权利、义务与责任。加强平台方的责任是互联网监管方式中效率较高的一种方式，立法应当设计科学、合理的平台责任制度，合理分配责任和义务，发挥平台方的专业和技术优势，提高网络监管效率；同时也不应过多加重平台责任，加重企

业运营的成本,影响企业创新与发展。互联网治理的复杂程度决定了无法单纯依靠政府和平台方的治理,而是要建立政府、市场、公民社会相互依赖与多元合作治理的模式。^①

(三) 以“自主可控”为目标,加强网络关键基础设施的安全和法律保护

网络空间的核心部分是国家关键基础设施。以美国为例,2013年美国制定了《国家网络安全和关键基础设施保护法案》(NCCIP法案),以加强16个关键基础设施领域和联邦政府的网络安全,强化基础信息系统建设、维护、防范等方面的监管。我国使用的信息基础设施和关键核心技术设备大量都是国外的,存在严重的“后门”威胁。“棱镜门”事件更是暴露国外主要智能操作系统服务商在其中扮演的角色。要实现我国网络空间安全的可管可控,保障关键基础设施安全,一是必须进一步推进以“国产替代”为主要措施的信息安全产业扶持政策,推动自主创新;二是要完善政府采购制度,对关系国家安全和公共安全利益的系统使用的重要信息技术产品和服务实施信息安全审查制度;^②三是立法要明确规范数据的收集、利用和跨境流动,建立可信任的数据安全保障机制,加强执法部门的定期核查。针对金融、能源、医疗、税收、财政等涉及重大公共利益的行业信息应当给予特别保护。

(四) 以前瞻性与现实性相结合为原则,提高互联网立法水平

互联网时代的治理需要立法者立足现实并具有前瞻性的眼光,以应对层出不穷的新技术、新应用带来的法律挑战和监管困境。在互联网环境下,立法所立足的技术背景和社会条件都处于急速的变化发展之中,法律的制定与实施既需要有前瞻性,以适应网络技术发展的日新月异,也要正视现实的可操作性,尽可能以相对稳定的法律规范去适应不断变化的网络环境。对于重点问题先行立法,使之有法可依,并在立法过程中,不断适应新形势,出台具体的管理细则。

① 杨乐:《平台责任制度与互联网合作治理》, <http://www.tencentresearch.com/Article/lists/id/2596.html>。

② 《中国将出台网络安全审查制度》, 新华网, http://news.xinhuanet.com/2014-05/22/c_1110811034.htm。



附表 我国信息安全相关法律与政策一览

政策			
1	《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号)	中共中央办公厅、国务院办公厅	2003
2	《关于进一步加强互联网管理工作的意见》(中办发[2004]32号)	中共中央办公厅、国务院办公厅	2004
3	《2006—2020年国家信息化发展战略》(中办发[2006]11号)	中共中央办公厅、国务院办公厅	2006
4	《关于加强网络文化建设和管理的意见》(中办发[2007]16号)	中共中央办公厅、国务院办公厅	2007
5	《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》	国务院	2012
6	《国家集成电路产业发展推进纲要》	国务院	2014
法律			
1	《刑法》	全国人大	1979
2	《全国人民代表大会常务委员会关于维护互联网安全的决定》	全国人大常委会	2000
3	《刑法修正案(三)》	全国人大常委会	2001
4	《中华人民共和国电子签名法》	全国人大常委会	2004
5	《中华人民共和国突发事件应对法》	全国人大常委会	2007
6	《中华人民共和国刑法修正案(七)》	全国人大常委会	2009
7	《中华人民共和国保守国家秘密法》	全国人大常委会	1988/2010 修订
8	《全国人民代表大会常务委员会关于加强网络信息保护的決定》	全国人大常委会	2012
9	《消费者权益保护法》	全国人大常委会	1993/2013 修订
国务院行政法规			
1	《中华人民共和国计算机信息系统安全保护条例》	国务院	1994
2	《中华人民共和国计算机信息网络国际联网管理暂行规定》	国务院	1996/1997 修订
3	《商用密码管理条例》	国务院	1999
4	《电信条例》	国务院	2000
5	《互联网信息服务管理办法》	国务院	2000/2012 修订
6	《中华人民共和国电信条例》	国务院	2000
7	《计算机软件保护条例》	国务院	2001
8	《中华人民共和国保守国家秘密法实施条例》	国务院	2014



续表

国务院部门规章及规范性文件			
1	《计算机病毒防治管理办法》	公安部	2000
2	《关于规范短信息服务有关问题的通知》	信息产业部	2004
3	《关于禁止发布含有不良内容声讯、短信息等电信信息服务广告的通知》	国家工商总局、信息产业部	2005
4	《非经营性互联网信息服务备案管理办法》	信息产业部	2005
5	《互联网新闻信息服务管理规定》	国务院新闻办公室、信息产业部	2005
6	《信息安全等级保护管理办法》	公安部、国家保密局、国家密码管理局、国务院信息化工作办公室	2007
7	《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》	国家发展改革委	2008
8	《电信业务经营许可管理办法》	工信部	2009
9	《电子认证服务管理办法》	工信部	2009
10	《互联网网络安全信息通报实施办法》	工信部	2009
11	《木马和僵尸网络监测与处置机制》	工信部	2009
12	《电子认证服务密码管理办法》	国家密码管理局	2009
13	《公共互联网网络安全应急预案》	工信部	2009
14	《通信网络安全防护管理办法》	工信部	2010
15	《关于加强工业控制系统信息安全管理的通知》	工信部	2011
16	《政府部门信息技术外包服务机构申请信息安全管理体系认证安全审查程序(暂行)》	工信部	2011
17	《电子认证服务业“十二五”发展规划》	工信部	2011
18	《移动互联网恶意程序监测与处置机制》	工信部	2011
19	《电信和互联网用户个人信息保护规定》	工信部	2013
20	《电话用户真实身份信息登记规定》	工信部	2013
21	《国家发展改革委关于加强和完善国家电子政务工程建设管理的意见》	国家发展改革委	2013
22	《关于加强移动智能终端进网管理的通知》	工信部	2013
23	《信息化和工业化深度融合专项行动计划(2013—2018年)》	工信部	2013
24	《关于开展深入治理垃圾短信息专项行动的通知》	工信部	2013
25	《即时通信工具公众信息服务发展管理暂行规定》	国家互联网信息办公室	2014
26	《关于进一步完善网络剧、微电影等网络视听节目管理的补充通知》	国家新闻出版广电总局	2014



续表

国务院部门规章及规范性文件			
27	《关于开展打击网上淫秽色情信息专项行动的公告》	全国“扫黄打非”办、国家互联网信息办、工信部、公安部	2014
28	《工业和信息化部关于加强电信和互联网行业网络安全工作的指导意见》	—	2014
29	《人口健康信息管理办法(试行)》	国家卫计委	2014
30	《关于进行信息类协议供货强制节能产品补充招标的通知》	中央国家机关政府采购中心	2014
31	《关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见》	银监会	2014
32	《通信工程建设项目招标投标管理办法》	工信部	2014
33	《打击治理移动互联网恶意程序专项行动工作方案》	工信部、公安部、工商总局	2014
司法解释			
1	《最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释(一)》	最高院、最高检	2004
2	《关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释(二)》	最高院、最高检	2010
3	《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》	最高院、最高检	2011
4	《最高人民法院、最高人民检察院关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释》	最高院、最高检	2013
5	《最高人民法院关于审理编造、故意传播虚假恐怖信息刑事案件适用法律若干问题的解释》	最高院	2013
6	最高人民法院、最高人民检察院与公安部联合出台《关于办理暴力恐怖和宗教极端刑事案件适用法律若干问题的解释》	最高院、最高检	2014
7	《最高人民法院、最高人民检察院、公安部关于办理网络犯罪案件适用刑事诉讼程序若干问题的解释》	最高院、最高检、公安部	2014
8	《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的解释》	最高院	2014