中国信息安全立法的宏观分析与制度设计探究

崔聪聪
（北京邮电大学 法律系，北京 100876）

摘 要：信息安全法的终极价值是自由。信息安全问题最终要依靠网络技术进步解决，因此信息安全法应保障和促进网络安全技术创新。绝对安全不具有技术上的可能性，或者要支付巨额的成本，因此信息安全立法应遵循适度安全和开放性原则，具体制度包括信息安全应急保障机制、信息安全监管、保障网络安全技术发展机制、网络安全意识培训和信息安全法律责任等制度。

关键词：自由；技术创新；网络安全

作者简介：崔聪聪（1978— ），男，河北深州人，法学博士，北京邮电大学法律系副教授，主要从事网络法研究。

基金项目：国家社科基金重大项目“国家网络空间安全法律保障机制研究”（项目编号：13&ZD181）的阶段性成果。

中图分类号：D913.4 文献标识码：A 文章编号：1001-4403(2014)01-0096-05 收稿日期：2013-10-10

互联网的和平与安全已成为世界各国共同面临的挑战。2010年5月27日，美国奥巴马政府发表的《国家安全战略》强调网络安全威胁是对国家安全、公共安全、经济安全最严峻的威胁之一。保护作为国家战略资产的数字基础设施与保护隐私权和公民自由一样，是维护美国国家安全的第一要务。①中国的互联网治理成就显著，但垃圾信息、制作和传播计算机病毒、网络欺诈、侵犯个人隐私、黑客攻击和网络恐怖主义等越来越多的网络滥用行为不断出现，其危害已发展到严重影响我国政治、经济、军事和文化安全的程度，同时也对个人权益造成了前所未有的威胁。出台信息安全法，保障中国的网络安全，已迫在眉睫。

一、中国网络信息安全现状

信息安全问题自古有之，只不过是在互联网出现后，这一问题被无限放大。网络颠覆了传统的信息交流环境，导致网络社会的信息安全问题较之传统社会更加复杂。与其他国家一样，信息安全已成为我国国家安全、公共安全和个人安全最严峻的威胁之一。

（一）国家安全受到严重威胁

网络运转是包括各种硬件设备和相应的软件在内的技术的有机结合，一旦离开了这些技术，网上活动将无法进行。就目前而言，从互联网资源到关键设备、网络核心技术和应用等都由以美国为首的西方国家所掌控，导致我国的网络安全岌岌可危。数据信息不仅蕴含着巨大的经济价值，而且隐藏着政治利益和国家利益，网络时代数据信息可能成为侵蚀他国主权和危害他国国家安全的一个强有力的武器。大数据时代，因各国的技术水平和收集、处理、控制数据的能力不同而导致信息流动出现了不对等：就经济、贸易信息而言，我国是典型的流出国，信息技术强国的信息“逆差”直接威胁着我国的经济主权和经济安全。

①见美国国家安全战略，2010年第27-28页。

?1994-2014 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

（二）公共安全受到严峻挑战

随着微博、SNS（社会性网络服务）的出现，信息在网上呈现瀑布式传播和扩散。上述网络创新应用所具有的强大的信息扩散力、渗透力可以将一般性局部事件快速演变为全局性的重大事件，使公共安全和社会稳定受到严重威胁。以美国为首的西方国家利用自身的网络技术和信息优势大量向我国灌输其意识形态和价值观念，恐怖组织、邪教组织、分裂势力积极借助网络空间攻击我国的社会政治制度，企图瓦解民族凝聚力，这直接威胁到党的执政地位和社会安全。此外，信息网络领域不断出现各种以渲染暴力恐怖为目的的文字、图片和视频，以侵害信息网络、破坏网络关键设施、侵犯公民人身财产权利的“恐怖主义”、“网络暴力”活动越来越猖獗，致使网络社会的公共安全受到严峻挑战。

（三）个人权益未获有效保障

数据信息已成为网络时代的重要资源。计算机网络所具有的强大的信息处理能力，导致个人信息被非法收集、利用以及泄露的损害后果更加严重，个人信息在网络时代受到了前所未有的威胁。苹果公司曾被曝在没有告知用户并获得许可的情况下，私自通过 iPad 和 iPhone 手机收集用户的行踪信息，经过处理后默认存储在一个未经加密的数据包中，每隔几个小时通过电信网或互联网成批发回苹果公司总部。DCCI 互联网数据中心发布的《2013 移动隐私安全评测报告》显示，有 66.9% 的智能手机移动应用（APP）在用户不知情的情况下抓取用户隐私数据，其中通话记录、短信记录、通讯录是隐私信息泄露的三个高危地带。

违法收集和滥用个人信息不仅侵犯了权利人的人格尊严，且往往是其他违法犯罪的工具和手段。近年来，通过违法收集、窃取等滥用他人个人信息的手段实现诈骗、盗窃乃至侵犯他人生命权的犯罪形式呈逐年上升之势。CNNIC 发布的《中国网民信息安全状况研究报告》显示，2012 年有 4.56 亿网民遇到过信息安全事件，占网民总数的 84.8%。在遇到信息安全事件的网民中，77.7% 的网民都遭受了不同形式的损失，除花费时间和精力外，经济损失总额为 194 亿元。

二、信息安全法的立法目的

立法目的是需要通过立法、执法和司法来实现的基本价值。信息安全法是在网络信息安全问题的不断恶化，已严重威胁国家安全、社会安定和个人合法权益的情况下，由此引起人们的关注并由此产生了解决网络信息安全的强烈需求和实现这一欲望或目的的法律规范。信息安全法的立法目的是指立法机关通过运用法律这种有效的社会调控手段确立一国的信息安全政策以及网络信息安全与发展的目标。

（一）美、俄信息安全法的立法目的

信息安全法的立法目的是一国在分析其国内特殊的网络安全形势基础上确定该国网络信息安全政策的具体体现。美国的信息安全战略经历了从主张“发展优先”到“安全优先”，从“适度安全”到“先发制人”，根据国家需求，构建了“信息基础设施保护”、“网络信息安全管理制度”和“信息安全文化与价值观”三位一体的国家信息安全战略体系。奥巴马政府出台的《网络空间国际战略》改变了以防御为主的网络空间战略，转而发展以“互联网自由”为核心，以“控制—塑造”为基本特征的进攻型网络空间战略。[1] 与国家的网络空间政策相适应，美国在本世纪之初的信息安全法的立法目的是防范网络攻击，保障网络安全，具体而言：减少美国对网络攻击的脆弱性，阻止针对美国至关重要的基础设施的网络攻击，在确实发生网络攻击时，使损害程度最小化、恢复时间最短化。[2] 可以预见，随着美国网络空间战略的变化，美国今后的信息安全立法乃至整个网络立法都会以实现控制为核心的进攻性网络空间政策为目标。

与美国不同，俄罗斯基于本国所面临的内在和外在的信息安全威胁，提出信息安全法的立法目的是：确保信息安全并在激烈的信息对抗中获得优势以维护国家利益。[3] 俄罗斯和美国信息安全法的立法目的之所以存在差异，原因在于信息安全法解决的是一国的特定问题，是与国内特定的信息安全形势相关的。因此，不同的国情决定了各国的信息安全立法有着不同的目的。

（二）中国信息安全法的立法目的

以安全威胁的来源为标准，可以将威胁我国信息安全的因素分为以下两类：一是网络核心技术失控；二是网络滥用行为。决定了我国信息安全法既要通过规制危害网络安全的行为，又要通过促进网络技术的发展以掌控网络的新技术从而保障我国的信息安全。具体而言，我国信息安全法的目的应通过设定各类主体（政府、网络用户、信息基础设施运营者和信息内容提供者等）的权力或权利、义务和责任，规范信息收集或生成、传递、控制和利用行为，促进网络基础理论的研究，

?1994-2014 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

掌控网络的核心技术，实现信息的保密性、完整性、可控性、可用性和不可否认性，从而有效地保障国家安全和个人在信息社会的基本权益。

安全主要体现工具性价值的特性又决定了它不可能被作为绝对的终极价值去追求[4]，信息安全法的终极目的是实现网络主体的自由。信息安全法通过构建并维持网络社会的基本秩序进而实现保障自由的目的。网络社会秩序究其本质是网络主体的一种有组织化的活动方式，是网络主体行使其权利的基础。自由只能在秩序中获得，这决定网络主体的自由必须依存于网络社会的秩序。自由不是个体的任意，恰恰相反，自由是对个别人的任意的超越和对普遍性的认同。[5] 信息安全法通过对危害信息安全的网络滥用行为的约束以保障其他网络主体的自由。

从社会学的视角看，信息是社会结构中不可缺少的构成性要素。[6] 14 大数据时代，数据信息进一步从社会资源中独立出来并成为一种新的结构性要素，对人类社会活动的各个领域发挥着深远的影响：数据信息对人类的政治、经济、文化等领域起到了基础性的支撑作用。鉴于信息在网络社会中的重要作用，信息安全法的目的应以实现信息的自由流动、保障网络主体传播和获取信息的自由为其终极目标。

中国已进入信息社会，网络之于中国公民的意义不仅仅是赋权、赋能，更重要的是赋信息。信息的自由流通能使人们进行独立思考并激发人们的创造能力。因此，网络不单单是信息传递的工具，而且是解放国人个性的工具。通过保障信息安全以促进信息自由流动，实现信息的最大化共享与利用；通过保障网络主体的行为自由，使其能够自由的传播和获取信息，从而激发网络主体的创造力。因此，信息安全法是提高国民素质，促进社会发展与进步，提升国家竞争力的重要制度保障。

三、中国信息安全立法的指导思想

信息安全立法的指导思想是指立法主体据以进行信息安全立法活动的重要理论根据，是为信息安全立法活动指明方向的理性认识。网络的开放性、全球性、虚拟性等特征以及信息安全立法的目的决定了我国信息安全立法应遵循以下指导思想。

（一）适度安全

绝对安全不具有技术上的可能性，抑或是要支付巨额的成本。不能为了获得绝对安全而不计成本，也不能因噎废食而放弃使用网络。因此，信息安全法的“安全”并非绝对安全，而应该是适度安全。适度安全是指信息安全法的制度设计应协调安全与其他价值之间的关系，不能为了保障信息安全而牺牲了网民的自由，进而扼杀了网络技术创新。网民可以在网络世界中自由地获取、传播、处理信息，这一权利已被我国宪法所确认，信息安全法律规范的制度设计不能因强调网络安全问题而影响网络的接入。原因在于，面对网络安全和信息安全问题，恐惧并不理智，不仅对问题解决没有效果，还可能导致过度控制。在个人生活和社会生活中，一味强调安全，只会导致停滞，最终还会导致衰败。[7] 401 因此，信息安全法应保证国内网民以及世界其他国家和地区的网民都有安全的接入机会。网络的可接入性应该有持续性的保障，除非发生危害国家安全的行为以及刑事犯罪行为。

整体安全和个人自由都是需要重点保护的根本利益，对任何一方保护的偏颇或疏漏都有可能造成整个信息安全法律关系的不稳定。因此，未来中国的信息安全法在保障整体安全的同时，应充分重视对网民个体自由的保护，在提升国家和政府对网络安全控制力的同时，协调好国家安全与公民个人自由之间的关系。

（二）开放性

云计算、移动互联网、物联网、大数据的出现将互联网发展带入一个全新的阶段，这对个人信息保护和国家安全保障提出了更高的要求。博客、微博、SNS 等网络新业务新形态的出现，移动通信技术的日益成熟和广泛应用，网络信息传播形式从以文字为主向音频、视频、图片等多媒体形态转变，不仅增加了监管的难度，而且使当事人之间的法律关系变得更为复杂。如果信息安全法律规范将有关范畴依附于某一特定的技术形态，而相关技术的发展则使得建立在先前某一特定技术基础之上的法律无法适应新技术条件下的网络活动。因此，信息安全立法应坚持开放性的原则，具有充分的前瞻性和预测性，保持适当的灵活性，避免将有关范畴局限于某一特定的技术形态而遗漏了对其他网络技术特别是网络创新应用的监管。

（三）依靠发展解决安全问题

安全问题最终要依靠网络技术进步解决，在此意义上，发展是解决安全问题的终极手段和措施。鉴于国内严峻的信息安全形势，决定了我国信息安全法既要侧重安全，又必须促进发展，依靠发展解决安全问题，在安全中求得发展。以网

?1994-2014 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

络攻击为例，利用最新的网络技术和应用可以有效地预防这一长期困扰行业健康发展的问题：通过对大数据的深入分析，能够帮助企业提前发现恶意进攻发起的时间，做出快速应对，制定智能驱动的安全策略，减少恶意攻击者的停留时间，建立以风险为基础、具备关联性、智能驱动的安全模型，帮助用户防御当今日益增长的高级威胁及恶意进攻者。

四、中国信息安全法的制度设计

信息安全法的立法目的是立法者将一定的价值观和法律理念在成文法上所做出的反应。遵循保障信息自由流通和网络主体行为自由的目的，中国信息安全法的具体制度设计如下：

（一）信息安全应急保障机制

网络技术的开放性特征决定了不可能消除所有的网络安全隐患，所以信息安全法的制度设计应具备最大限度地避免危害信息网络安全行为的发生以及最大限度降低网络安全事件引发的损失的功能。美国在2003年启动了爱因斯坦计划，其系统能够自动地收集、关联、分析和共享美国联邦国内政府之间的计算机安全信息，使得各联邦机构能够接近实时地感知其网络基础设施面临的威胁，并具有对恶意行为的分析能力，在上述基础上识别并标记恶意网络传输，从而能够自动地检测网络威胁并在危害发生之前做出适当的反应，有效地提升了网络安全保障能力。因此，建立信息安全应急保障机制应成为信息安全法的核心内容。

信息安全应急保障机制包括应急管理机构的设置及其职权、安全信息分析与共享机制、信息安全应急预警机制及其程序、因应急保障机制启动而对公民、法人及其他组织的权利限制及其私权遭受损害时的救济措施、紧急情况下未及时报告或隐瞒、谎报等违法行为的法律责任等。应急反应的主体包括政府组织、社会应急服务机构和网络运营单位，针对不同性质的应急反应机构规定其承担不同的义务。建立由国家主管信息安全的最高领导人负责，公安、安全、保密、机要、电信和军队等执法、管理或者重要领域部门的负责人参加的协调机构，发布或终止国家或区域性的紧急状态命令。明确国家计算机网络应急技术处理协调中心的法律地位和职责，为政府机构和企事业单位的信息系统的安全管理人员提供及时的技术帮助，包括检测和处理信息安全事件方面的指导；汇总和分析有关威胁信息安全的事件的信息；通知各机构信息系统的安全管理人员目前和潜在的信息安全威胁和缺陷。

（二）信息安全监管制度

在信息安全法中明确以政府为主导、行业组织和社会共同监管的信息安全监管模式，并明确各监管机构的职责。规定信息安全监管机构应当对其他政府机构和企事业单位的信息系统和信息安全保护措施进行评估的程序以及对上述机构执行信息安全管理规章制度的情况进行监督的程序和处罚措施。同时鼓励行业组织、技术联盟通过制定行业规则、技术标准等手段，加强对信息安全的监管。

（三）促进我国网络安全技术发展的机制

互联网是一个依托先进信息技术的全球性基础设施，因此保障网络安全不能仅仅依靠法律和行政手段，还必须以强有力的安全技术作为支撑。经过数年持续不懈的努力，中国互联网内容监管技术已发展到了一个非常成熟的阶段，通过多手段、多途径、多层次、分布式的处理，把大多数网民能接触和传播的信息控制在一个政府能接受的水平。[8] 但网络安全技术研发的高成本、长周期、低回报等客观因素，造成企业缺乏投资热情，这就需要政府进行投入，以提高网络企业进一步投资的信心。我国很少有实力强大的研发网络安全产品的企业，只有国家成为网络安全投入的主体，才能生产出技术含量高的内容过滤软件、杀毒软件、防黑客软件等安全技术产品，建立网络安全运行的技术保障体系。

美国是信息技术强国，凭借其先发优势，已经产生一些具有国际竞争实力的网络安全技术研发企业，比如赛门铁克等，美国政府大量的资金投入从中起到较强的推动作用。2002年2月，美国众议院通过了《网络安全研究与发展法》，该法在机构建设、研究计划管理、资金投入与管理、专门人才培养等方面确立了保障美国国家信息安全的具体制度。依照该法的规定，美国2003—2007财年共投入2.33亿美元专项研究经费用来研发网络安全技术。

借鉴美国的成功经验，我国应以法律的形式认可向计算机和网络安全的研究提供资金支持，规定资助的范围、基金的申请条件和程序以及奖励机制。成立专门的机构，通过分析现有网络技术的缺陷，制订详细的资助计划，有针对性地支持进行网络信息安全研究的科研机构。对于网络的核心技术和网络的基础协议，应投入专门的经费进行研究，具体包括网络、系统、设备、终端、应用软件等方面在内，特别要把网络安全技术（包括认

?1994-2014 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

证、加密、入侵检测、漏洞评估和检测、远程访问控制以及其他安全数据通信技术）研究放在优先位置，从网络核心到网络末梢等各个环节的技术和应用应做到重点突出、自主创新、自我掌控。

（四）网络安全意识培训

在新兴的信息社会，每个人都是信息的生产者和消费者，每个人都有营造安全、可靠的网络环境的义务。欧盟关于建立欧洲网络信息安全文化决议要求每一个参与者都是保证安全的重要角色。[9] 因此，保卫中国的网络空间需要所有中国人的行动，包括最普通的大众。任何成功增强网络安全的国家力量必须是提高全体国民的安全意识（各个层面的使用者和管理者）。①网络安全教育可以为网络安全形成一个保护层，是信息社会的基石。因此，国家应重视公民网络安全意识的培养，以法律的形式制订培训公民网络安全意识的国家计划和方案，使社会公众认识到中国经济和国家安全对计算机和信息系统依赖的程度，唤醒公众积极采取行动保护国家网络的意识，以支持网络安全的需要。开展系统化的公众网络基础素质教育，对社会公众进行有关网络道德和正确使用互联网和其他通讯方式的教育，使公众意识到保障信息安全的重要性，从而积极配合政府监管措施的实施。社会公众网络安全意识和网络基础素质教育是一个长期的过程，应建立从小学、中学到大学以及在职教育和社区层面的系统化和终身化的教育体系，构建自上而下和自下而上双向进行的教育模式，创造一个由法律保障的全民参与、保障网络安全的体制，使社会公众参与并确保他们拥有的、操作的、控制的或用于联结的网络空间的安全。

（五）信息安全管理人员的培训

信息安全管理具有很强的技术性和专业性。从政府、企业到社会组织和公众对于信息安全管理专业人员都有非常强烈的需求。人才的匮乏不仅影响了网络的应用，更影响了政府部门的舆情分析、宏观决策的科学性以及公众合法权利的保护。因此，对现行网络管理人员进行信息和通信技术、安全问题和相关法律知识等专业化培训，使网络监管人员充分了解信息通信技术本身的危险及其被滥用的情形，理解信息通信技术相关的风险、网络威胁和网络攻击，提高监管部门和监管人员的监管能力，实现互联网新业务和相应监管能力同步发展的良性局面。

（六）信息安全法律责任制度

现行网络法律中很少有网络服务提供者的义务和责任的规定，网络信息安全的风险最终由用户承担，在一定程度上助长了网络安全事件的发生。为有效地防范信息安全事件的发生，最大限度地降低网络安全事件引发的损失，信息安全法应规定网络的运营者、使用者和所有人必须成立专门的保障网络信息安全的机构，评估未经授权进入、使用、披露、破坏、修改和毁坏信息或信息系统所造成的危害和风险，制定相应防范信息安全风险的规章制度。定期测试信息安全政策、程序的有效性和评估信息安全控制和技术，确保其得到有效实施。信息安全义务主体未履行相应的保障信息安全的义务时，应承担相应的法律责任。未及时发现和修复信息系统的安全缺陷，使自己的网络成为第三方恶意攻击的路径而导致他人的合法权益遭受损害时，信息安全义务主体应对他人承担损害赔偿责任。此外，信息安全法应根据违法行为的社会危害性（破坏不同领域的计算机网络信息系统）不同，设定不同的法律责任形式（行政责任或刑事责任）。

①见美国网络空间安全国家战略，2003 年第 38 页。

参考文献

[1] 傅荣校．国家信息宣全理念与信息安全能力建设 [J]．信息安全，2012，(7)．

[2] 马民虎．信息安全法律体系 ：灵魂与重心 [J]．信息网络安全，2007，(1)．

[3] 马民虎．信息安全立法三论 ：价值、范围和原则 [J]．信息网络安全，2005，(3)．

[4] 马民虎，李江鸿．我国信息安全法的法理念探析 [J]．西安交通大学学报（社会科学版），2007，(3)．

[5] 龙文懋．“ 自由与秩序的法律价值冲突 ”辨析 [J]．北京大学学报（哲学社会科学版），2000，(4)．

[6] 李晓辉．信息权利研究 [M]．北京 ：知识产权出版社，2006.

[7] E. 博登海默．法理学 ：法律哲学与法律方法 [M]．邓正来，译．北京 ：中国政法大学出版社，1999.

[8] 李永刚．中国互联网内容监管的变迁轨迹——基于政策学习理论的简单考察 [J]．南京工业大学学报（社会科学版），2007，(2)．

[9] 马民虎，王新雷．我国信息安全法律能力建设的思路 [J]．信息网络安全，2010，(9)．

［责任编辑 ：康敬奎］

?1994-2014 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net