【网络法·网络安全法专题】

我国网络安全管制的基础、架构与限定问题

——兼论我国《网络安全法》的正当化基础和适用界限

龙卫球

(北京航空航天大学　法学院,北京　100191)

[摘　要]　我国《网络安全法》奉行着一种关于网络安全治理的强监管理念,在当今世界的网络安全专门立法中可谓独树一帜,系以一个更加多层次的综合化的网络安全概念为面向,重在强化国家对于网络安全的管制力。其体系架构,在原则上体现为一种由复杂原则组合指导的特点,但格外强调国家管理的本位性和直接性;在管制事项上则体现为名目繁多,内容绵密,并呈现不少独特的体制特色。所以,为了有效而合理地实施《网络安全法》,应当深刻理解有关网络安全管制正当化基础及其演化,更加准确地解读和把握我国网络安全管制的内在基础和外在边界,并且还要特别注意实施中的目的体系、行政权属性以及网络技术架构等限定问题。

[关键词]　网络安全法;网络安全管制;管制框架;正当化基础;适用限定

[中图分类号]　D9　　[文献标识码]　A　　[文章编号]　1000－5072(2017)内熔0001－13

• z!–Ìz!JÈËññÂÀ

[收稿日期]　2017－01－26

[作者简介]　龙卫球(1968—),男,江西吉水人,北京航空航天大学法学院教授,教育部长江学者特聘教授,法学博士,主要从事民商法、信息法研究。

[基金项目]　国家社会科学基础重大项目《信息法基础研究》(批准号:16ZDA075)。

! 关于主要国家网络安全立法的介绍,可参见沈玲、何波《网络安全》,中国信息通讯研究院互联网法律研究中心、腾讯研究院法律研究中心主编《网络空间法治化的全球视野与中国实践》,北京:法律出版社 2016 年版,第 140—145 页。

主体、共享方式、实施和审查监督程序、组织机构、责任豁免及隐私保护规定等,同时通过修订纳入 2002 年《国土安全法》的相关内容,规范国家网络安全增强、联邦网络安全人事评估及其他网络事项。欧盟在 2016 年 7 月 6 日由议会正式通过了《网络与信息系统安全指令》,8 月 8 日正式生效,责令欧盟国家必须在此后 21 个月内转化为国内法,并确立了多项制度,包括:实行网络与信息安全国家战略管理、增强欧盟国家间网络安全战略合作与跨境协作、建立计算机安全事件响应团队,并建立欧盟合作网络、区分基本服务运营者和数字服务提供者分别赋予的不同监管义务(前者为重监管,后者为轻监管)、针对不同主体建立不同程度的网络安全事件报告制度、鼓励产业发展并将小微企业排除监管之外等。

我国在 2016 年 11 月 7 日出台了《网络安全法》,2017 年 6 月 1 日起正式施行,堪称一部全面规范网络空间安全管理方面问题的基础]茵　间题　　0]蜕　粹　+蜡　~　⑾的　!<粹　L邵.{　,娀)　仕潟

马病毒)等,到通过网络或介入网络,针对他人的财产、人身进行攻击、侵害甚至犯罪。所以,对于网络安全问题,不能局限于事实层面而应该深入到利益关系中去思考。网络技术和应用发展到一个阶段之后,特别是随着网络空间不断社区化、商业化乃至实境化,网络空间滋生出各种利益关系且不断复杂化,网络空间与真实空间的互动也日趋密切,网络空间安全问题也同样影响越来越大。关于应对网络安全问题的意识随着网络安全事件不断升级也就不断得到强化。[!] 按照美国政府在关于网络安全的立法建议中的说法,当今时代网络和计算机安全之所以被认为十分重要,其原因至少体现在两个方面:一是信息技术进步和电子商业发展越来越扮演重要的作用,使得网络安全成为经济的一个关键要素;二是网络安全对于美国应急反应等安全系统和国家能源设施等关键系统来说,已经至关重要。["]

人们虽然相信网络安全重要,但是对于是否需要专门赋予政府一套网络安全管制权力,却一直存在疑虑,担心一旦允许国家以网络安全为名建立专门的管制,把握不好可能会变成一种国家对于网络空间的任性管理。这里,产生疑虑的原因,既有管制理论上的困惑,更有现实中对于政府可能借用安全问题而擅用扩权的畏惧。所以,很长时期以来,一种观点认为,网络安全的治理不应该有特殊性,从管制基础和范围来说,只需将一般法律关于安全的治理规则推及网络空间即可,这些法律如国家安全法、刑法、侵权法中的有关安全的规则等,没有必要通过专门立法来确立一套所谓的网络安全专门管制体系。这种观点反对专门的网络安全立法,认为这样只会导致任意增加政府权力而没有效率,进而添加网络负担,甚至妨碍网络发展。例如,来自美国网络信息技术机构的代表和网络政治家就激烈反对政府管制论,美国信息技术协会主席 Harris Miller[#]、TechNet 的总裁 Rick White[$] 等呼吁,在所谓网络安全问题上,过多的政府规制会对网络企业通过革新提升网络安全能力带来阻碍或限制,或者影响其灵活性。所以,美国国会和联邦政府早期虽然试图发起一些网络安全管制方面立法,但是多数没有成功,那些立法议案失利的主要原因,是遭到网络企业代表等方面对政府管制的警惕和反对。[%]

遗憾的是,网络安全的恶性事件不断,特别是在 2010 年之后大量的全球范围网络安全事件的发生和带来的巨大破坏,促使人们反思:仅仅寄希望于网络企业和民间力量似乎是不够的,在市场力量和政府力量之间应该有所平衡。此外,2013 年斯诺登事件出现之后,人们甚至一些国家政府还意识到,网络安全治理需要应对的,还有国家任意行为问题,网络安全管制包括对国家行为的管制。在这种背景下,主张通过专门的网络安全立法,确立国家和政府主导的管制体系以有效应对网络安全问题的观点,逐渐占据上风。这些观点,有的是从网络活动的价值追求和利益保护的角度,有的是从管制技术效用的角度,有的则是从其他的正当化辨识角度,支持通过立法建立政府主导的网络安全管制体系。例如在美国,政府官员和网络安全专家,包括著名的 Richard Clarke[&]、Bruce Schneier[']、Rick Boucher[(] 等,就属于力推政府应当介入网络安全管制的代表人物,他们极力主张应当通过建立政府特别管制来提升网络安全。他们认为,私有机构已经失败于自己解决网络安全问题,所以需要引入政府的规制,通过具有威胁性的规则或者经济刺激等办法,以便让私有机构有压力或动力去采用或写出更加安全的软件或代码。最终支持加强政府管制的观点,在世界范围推动了一轮网络安全立法,主要网络国家包括日本、美国、欧盟等,2014 年之后纷纷做出立法决断,纷纷出台专门的网络

! 参见关于网络安全的历史,参见 Ted Julian, "Defining Moments in the History of Cyber-Security and the Rise of Incident Response. All the milestone incidents from the past 25 years",https://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/,最后访问时间:2017 年 2 月 16 日。

" 参见 Kirby, C., "Forum focuses on cybersecurity"(December 4, 2003). ,San Francisco Chronicle; "Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure",updated: 2012-07-26. New York Times; Homeland Security,Written Testimony of U.S. Department of Homeland Security Secretary Janet Napolitano for a Senate Committee on Homeland Security and Governmental Affairs hearing titled "Homeland Threats and Agency Responses", https://www.dhs.gov/news/2012/09/19/written-testimony-secretary-napolitano-senate-committee-homeland-security-and,最后访问时间:2017 年 2 月 13 日; Marshall Brain & Wesley Fenlon, "How Computer Viruses Work",http://computer.howstuffworks.com/virus.htm,最后访问时间:2017 年 2 月 13 日。

参见"Harris Miller",https://en.wikipedia.org/wiki/Harris_Miller,最后访问时间:2017 年 2 月 13 日。

$ 参见"Rick White",https://en.wikipedia.org/wiki/Rick_White_(politician),最后访问时间:2017 年 2 月 13 日。

% 这种观点非常强势,导致了美国联邦许多网络安全相关立法的流产。参见维基百科 "Cyber-security regulation",https://en.wikipedia.org/wiki/Cyber-security_regulation#endnote_kirby,最后访问时间:2017 年 2 月 13 日。

& 参见"Interview Richard Clark", http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/clarke.html.

' 参见"Schneier on Security", https://www.schneier.com/blog/about/,最后访问时间:2017 年 2 月 13 日。

(参见 Menn, J. "Security flaws may be pitfall for Microsoft", Los Angeles Times updated: 2002-01-14。

安全法,尽管架构和范围不尽相同,但都呈现了一种强化政府管制权力的趋势。我国 2016 年《网络安全法》也是在这股浪潮中应运而生,旨在通过确立强大的政府管制手段,以便应对当下非常复杂、非常重要的网络安全治理需要。

三、我国网络安全管制架构: 概念、原则和事项的分析视角

我国《网络安全法》的治理基础,系以一个更加多层次的综合化的网络安全概念为面向,重在强化国家对于网络安全的管制力。其架构原则,体现为由复杂原则组合指导的特点,一定程度上考虑了网络技术和组织特点而照顾多样化协同治理的需要,但关注点在于如何指导构建一套体现国家地位的强管制架构; 其管制事项,名目繁多,可谓体系广泛而内容绵密。

(一)《网络安全法》管制的概念面向

《网络安全法》既以管制"网络安全"作为对象,可见该概念的界定处于体系解释的中心位置。《网络安全法》第 76 条对"网络"和"网络安全"进行了法律界定,意在避免法律适用的模糊性。即,"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。""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。"该条关于网络安全的定义方式,是一种技术事实层面的描述,立足网络安全实施主体的行为和能力的角度。这一定义与我们见到的欧盟指令(NIS Directive)的相关界定极为近似,[!]应该说这是一种比较可观、容易把握的定义。

从法理上来说,这个定义存在进一步加以解释限定的必要,因为该定义所称的网络安全,实际上并不是简单的行为事实(攻击、侵入等)或者技术事实(数据完整性、保密性、可行性等)就够,还存在所要防范和所要保障的对象限定问题。试想,那些客观上或主观上与法律利益完全没有关系的网络安全,对我们来说应该并无意义,那还需要落入到本法所谓的网络安全范畴吗? 当然应该排除。网络安全法作为一部法律,其所谓的网络安全,是要从法律体系出发追求法律意义的,所以应该进一步地限定为与法律利益具有相关性,即与法律利益保护结合起来,是一种涉及法律利益保护目标的网络安全。也就是说,网络安全不只是某种绝对单纯的技术安全或行为安全,而应该是网络空间产生的或带来的与法律利益息息相关的网络安全,这些法律利益或者存在于网络空间本身,或者透过网络介入或者活动而被连接到。

从概念使用内涵上来说,应当注意我国"网络安全"十分复杂和独特,存在准确理解的必要。首先,和其他国家一样,网络安全概念,需要借助相关的知识和规范加以补充丰富。["] 例如,网络安全应该包括网络物理安全和信息安全两个方面。网络安全法出台前,我国法律政策文件多使用"网络与信息安全"的表述,如《国家安全法》使用的就是"网络与信息安全"。但应注意信息安全是重心所在,作为网络的传输、应用对象,网络信息的安全性问题必然构成网络安全问题的核心部分。狭义的信息安全强调的是防止不良的外来信息的入侵,防止信息的泄漏、修改和破坏等等。广义的信息安全既有网络的运行安全(防止入侵),也有信息本身的安全(信息加密等),也间接包括构成网络的设备本身的安全。此外,《网路安全法》还可从网络安全的行为或实现环节加以理解,因此隐含了技术安全、管理安全、内容安全的区分。另外,我国《网络安全法》和其他国家一样,也及时关注了数据时代的网络数据安全问题。网络安全存在数据安全的升级问题,网络安全本质上是一个具有发展属性的概念,其中数据安全成为当前网络安全规制与重点关注的新代际问题。

其次,非常重要的,是我国关于网络安全的概念,比较起其他国家来,[#]具有更加多层次、多角度的内涵特点,因此更加具有广泛性,这就使得我国关于网络安全的理解范围其实更加宽泛和独特,我国《网络安全法》

[!] 2016 年欧盟《网络与信息系统安全指令》所界定的"网络与信息系统安全"是指"在一定可信水平下,网络与信息系统抵抗破坏其所存储、传输、处理之数据或者相关服务的可用性、真实性、完整性或者保密性行为的能力"。参见 The Directive on security of network and information systems(NIS Directive), Art. 4, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive,最后访问时间: 2017 年 2 月 15 日。

["] 参见龙卫球、林桓民《我国网络安全立法的基本思路和制度建构》,《南昌大学学报》(人文社会科学版)2016 年第 2 期。

[#] 美国学者中比较流行的看法认为,网络空间与真实世界存在主权竞争关系,这使得网络空间的主权问题与真实世界国际法上的主权问题比较起来显得微妙,我们应当重点关注的是如何处理好这种竞争关系。参见[美]劳伦斯·雷席格著,刘静怡译《网络自由与法律》,台北: 台湾商周出版社 2002 年版,第 465 页。

的实际管制空间因此更加宽泛。2016 年 12 月我国首份《国家网络空间安全战略》出台,明确使用了网络空间存在政治安全、经济安全、文化安全、社会安全和国际安全的分类描述。政治安全针对网络渗透,经济安全针对网络攻击,文化安全针对网络有害信息,社会安全针对网络恐怖和违法贩子,国际安全指网络空间的国际竞争。[!] 其中,非常值得重视的,是我国关于网络主权安全的意识。我国特别强调,要从网络主权高度来看网络安全,没有网络安全就没有国家安全,["] 认为随着全球信息化的深入发展和持续推进,以数字化、网络化、智能化、互联化、泛在化为特征的网络社会逐渐向国际空间化方向发展,为网络安全带来了主权空间化意义的新内涵。[#] 所以,在我国网络安全中,很注重一般安全和网络主权安全(属于国家安全的重要部分)的区分,[$] 网络空间安全成为我国主权安全观念的新领域,也是我国国际关系观念的新领域。[%]

(二)我国《网络安全法》管制的架构原则

《网络安全法》在管制架构上体现出一种由多项原则复杂组合指导的特点,包括统一管理和分工协作结合、战略管理与具体管理结合、社会共治、国际协同合作、加强未成年人等特殊保护等。我国的这些原则组合,与其他国家比较有许多相同点,比如也重视战略管理、协同共治、区分特殊保护等,但是也有不少专属于自己的体制和观念特色,尤其是特别注重凸显国家管理架构。

1. 统一管理和分工协作结合

旨在使网络安全管理与网络安全事项本身的层级性和复杂多样性相适应。体制上,既有担当统筹、协调、监督的统一权威架构,即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,又有从合理分工需要、现有职权配置和分层的现实出发的区分式具体管理架构,即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,同时规定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。[&]

2. 战略管理与一般管理结合

《网络安全法》引入了网络安全的战略管理体制,应对网络安全治理需求。《网络安全法》第 4 条规定:"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。"当前各国无一例外将网络安全问题上升到国家战略高度,我国也毫不例外。这种战略管理权与其他为数不多的一些领域的战略管理权一样(例如国防军工、航空航天等),是一种国家得高度干预网络空间的一种抽象治理权力。网络安全治理上升到战略的正当性和必要性在于:网络安全治理体系不同于一般治理体系,网络安全对于所置身的网络信息化事业本身具有战略基础价值,是关系国家网络事业发展、维持和强化国家竞争力的基础和保障,因此网络安全治理本身也同样必须具备与这种基础性相匹配的战略高度。这种网络安全战略的权力,究其范围,虽然智者见智仁者见仁,但不是绝对的,而是体现为目标引导、关于重点领域的安全政策、特定的安全支持和促进措施等。网络安全战略通常是防御性的,但为确立威胁必要也有进攻性的,包括通过提升进攻性网络能力和加密技术等应对网络恐怖,打击严重的网络犯罪,适时反击国外敌对活动。[']《网络安全法》同时也规定了一般管理,主要体现为网络运行管理(重点为关键信息基础设施管理)、网络信息安全、监测预警与应急处置等内容。

! 参见国家网络信息办公室《国家网络空间安全战略》,http://www.cac.gov.cn/2016-12/27/c_1120195926.htm,最后访问时间:2017 年 2 月 17 日。

" 参见《习近平在 2014 年 2 月 27 日主持召开中央网络安全和信息化领导小组第一次会议时的讲话》http://www.cnitsec.com.cn/index.php/index/articontent/menuid/13/tabid/39/classid/0/id/3144/type/news.html,最后访问时间:2017 年 2 月 17 日。

王世伟《论信息安全、网络安全、网络空间安全》,《中国图书馆学报》2015 年第 2 期,第 75—76 页。

$ 《国家网络空间安全战略》明确提出,我国国家主权的新疆域包括网络空间。参见国家网络信息办公室《国家网络空间安全战略》http://www.cac.gov.cn/2016-12/27/c_1120195926.htm,最后访问时间:2017 年 2 月 17 日。

% 国内网络主权观念又可区分为积极主权和消极主权两种不同观点。参见龙卫球、赵精武《我国网络安全规制的治理思维与架构》,中国互联网协会主编《互联网法律》,北京:电子工业出版社 2016 年版。

& 参见《网络安全法》第八条。

' 参见《英国新版《网络安全战略》彰显雄心》,搜狐网,http://mt.sohu.com/20161112/n473017982.shtml,最后访问时间:2017 年 2 月 13 日。

3. 多方共同治理

鼓励政府部门、网络运营者、网络行业组织、用户等多方共同参与,根据各自的角色参与到网络安全治理工作中来。政府和网络运营者共治是网路空间治理的共识,因为网络空间具有建立在代码基础上的架构特殊性,所以网络安全管制仅仅依靠政府单方面的行为往往无法实现,必须开展政府与网络企业或机构的合作。[!] 《网络安全法》接受了这种观念,为此规范了网络运营者的共治义务,强调网络运营者自身必须遵循合法运营和标准化经营要求。["] 同时,《网络安全法》基于网络活动和行为多主体的复杂性,还从增进管制效率出发,确立了网络利益相关者共同参与网络安全的保障义务。[#]

4. 国际合作治理

目标在于推动构建一个和平、开放、安全的国际网络空间。[$] 网络空间日益成为各个国家重要的战略资源,也成为各国交往和利益博弈的重要空间,随着网络技术不断革新,网络应用不断国际互通,网络安全威胁包括网络违法犯罪的安全威胁日趋国际化,网络威胁日益成为全球性难题,网络安全问题显然很难依靠一个国家解决,需要利益相关方国际共同配合。[%] 所以,网络安全的国际合作成为必要,不仅是为了平衡好网络空间中各国的利益,更为重要的是需要通过合作创造和保障安全的共同网络环境。我国通过此次立法承诺,以积极的姿态,包括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网络安全国际交流与合作,来推动构建和平、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。[&]

5. 强化对未成年人特别保护

就特殊利益的网络安全,应建立特别的保护机制和规则。《网络安全法》对未成年的身心健康活动给予了高度的关注,强调对未成年人应当进行特殊保护。第十三条规定"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。"遗憾的是,我们目前对于国外特别关注的电信领域用户通信自由和秘密安全特殊保护问题尚未足够关注,期望在接下来的电信立法中得到关注和改进。

(三)《网络安全法》管制的架构事项

《网络安全法》在管制事项上布局绵密,建立了丰富的管制渠道,授予政府和有关方面广泛而刚性的权力,构成了一个形式庞大的权力集群。

1. 网络安全的战略管理

《网络安全法》在总则第四条确立了国家就网络安全具有战略管理权力。其主要内容可以通过制定并不断完善网络安全战略的方式,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。2016 年 12 月 27 日,国家互联网信息办公室经中央网络安全和信息化领导小组批准,发布了我国首份《国家网络空间安全战略》,确立了总体目标、原则和战略任务。其中,目标为"推进网络空间和平、安全、开放、合作、有序,维护国家主权、安全、发展利益,实现建设网络强国";原则包括尊重维护网络空间主权、和平利用网络空间、依法治理网络空间、统筹网络安全与发展;战略任务包括坚定捍卫网络空间主权、坚决维护国家安全、保护关键信息基础设施、加强网络文化建设、打击网络恐怖和违法犯罪、完善网络治理体系、夯实网络安全基础、提升网络空间防护能力、强化网络空间国际合作等。[']

2. 网络安全的支持与促进

《网络安全法》专章对促进与支持网络安全,设定了国家和政府相关的一些措施权力。此处涉及"国家"表述时,意味着立法机构、行政机构、司法机构均有相应职权。这种国家依法具有的可以采取促进和支持措施的权力,观念上其实可以归属于战略权力的层次,是与战略贯彻直接相关的一类重大权力。

! 参见[美]劳伦斯·雷席格著,刘静怡译《网络自由与法律》,台北:台湾商周出版社 2002 年版,第 79 页。

" 参见《网络安全法》第九条、第十条规定。

《网络安全法》第六条强调净化网络环境和鼓励社会监督;第十一条明确行业自律在网络安全保障中的重要地位;第十二条规定了依法使用网络的权利以及守法、遵守公共秩序和尊重社会公德的要求;第十四条规定个人和组织的举报义务。另参见"谢永江:《〈网络安全法〉专家笔谈》",http://law.law-star.com/cac/4360137320.htm,最后访问时间:2017 年 2 月 17 日。

$ 左晓栋《网络安全法(草案)评述》,《中国信息安全》2015 年第 8 期。

% 崔聪聪《〈网络安全法〉专家笔谈》,http://law.law-star.com/cac/4360137320.htm,最后访问时间:2017 年 2 月 17 日。

& 参见《网络安全法》第七条。

' 参见国家网络信息办公室《国家网络空间安全战略》。

我国《网络安全法》赋予的此类权力,包括:(1)国家具有基于促进和支持网络安全需要的标准化的权力。体现为通过网络安全的标准化建设,促进网络安全。[!] (2)省级以上政府具有通过统筹规划、支持研发、保护知识产权和支持创新等促进网络安全技术的权力。["] 这种权力扩及到网络数据安全保护和利用的技术。[#] (3)国家还被赋有推进网络安全社会化服务体系建设的权力。体现为认证、检测、风险评估、支持管理创新等手段。[$] (4)国家还具有开展安全宣传和支持网络安全人才培养的权力。[%]

3. 网络一般运行的安全保障

《网络安全法》第 3 章第 1 节规范网络一般运行安全,赋予了国家相关的网络运行安全保障权力。具体包括以下保障权力:

(1)国家实行网络安全等级保护。(第二十一条)(2)网络产品、服务提供者应当承担网络安全保障若干义务。(第二十二条)(3)网络关键设备和网络安全专用产品实行安全认证合格或者安全检测。(第二十三条)(4)网络运营者应当要求用户提供真实身份信息。(第二十四条)(5)网络运营者应当制定网络安全事件应急预案,及时处理安全风险。(第二十五条)(6)国家保障开展网络安全认证、检测、风险评估等活动,向社会发布网络安全信息,应当依法进行。(第二十六条)(7)国家保障任何个人和组织禁止从事危害网络安全的活动,禁止提供危害网络安全活动的程序、工具或明知的帮助。(第二十七条)(8)国家保障网络运营者应当为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。(第二十八条)(9)国家支持网络运营者之间通过合作提高安全保障能力,支持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等。(第二十九条)(10)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。(第三十条)

《网络安全法》在网络一般运行安全要求方面,比较其他国家和地区的规定,确立了较多的管理权力和刚性义务,因此导致网络经营者和用户较重的负担。例如在欧盟指令(NIS Directive),其适用于数字服务提供者的网络安全监管义务,相当于我们的网络一般运行安全义务,总体上较轻且具有灵活性(关于与程度适应的要求),多属于事后监督。[&] 欧盟指令还特别鼓励小微企业(工人在 10 ~ 50 人之间,且年营业额或资产总额在 200 万 ~ 1000 万欧元之间为小型,之下为微型)的发展,将之排除在监管之外,明令对于数字服务提供者的网络安全监管义务不适用于小微企业。[']许多国家包括欧盟、美国也没有像我国《网络安全法》第二十八条那样宽泛规定一种为依法维护国家安全和犯罪侦查而提供技术支持和协助的义务。[(] 我国《网络安全法》第二十四条关于实行实名制的规定,在立法过程中更是争议颇多,而韩国在 2012 年就通过宪法法院的一个著名判决推翻了实名制要求,认为实名制或者说身份认证虽然是控制网络安全的一种有效手段,但是另一方面却也可能成为妨碍网络自由、威胁个人信息等的原因。[)]

! 参见《网络安全法》第十五条规定。

" 参见《网络安全法》第十六条规定。

参见《网络安全法》第十八条规定。

$ 参见《网络安全法》第十七条规定。

% 参见《网络安全法》第十九条、第二十条规定。

& 参见 NIS Directive,第四、五、十四、十五、十六、十七、十九、二十条。总体上来说,欧盟指令 NIS 纳入监管的数字市场主体分为“基本服务运营者”(operators of essential services,包括能源、运输、银行、金融市场基础设施、医疗卫生领域、茵] [　　管┼ZI始瘟兼收

'

(

)

4. 关键信息基础设施运行的安全保障

各国都将关键信息基础设施视为网络安全保障的核心部分。这是因为关键信息基础设施不仅对于具体的运营者和用户而言,而且对于整体的经济安全、社会安全甚至对于国家安全而言,都具有至关重要性,并且与国家安全和社会公共利益息息相关,因此国家重点保障其运行网络安全非常必要。[!] 美国在 2015 年《网络安全法》(该法重点网络安全信息共享制度)之前,就将关键基础设施视为网络安全核心的组成部分,联邦立法虽然一直在努力,但是进展并不顺利。["] 白宫在 2014 年初发布《促进关键基础设施网络安全的框架》,提出了实际操作和相关技术标准的指引,成为全球典范。

我国《网络安全法》与其他国家一样,特别强调保障关键信息基础设施运行的网络安全的要求。第三十一条对"关键信息基础设施"采取了列举加限定的办法,为"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",并且授权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。从比较法上看,不同国家对于"关键信息基础设施"范围理解并不一致,但大都是从自身据以为国计民生的角度来界定。比如,欧盟界定为能源、运输、银行、金融市场基础设施、医疗卫生领域、饮用水供应及分配、数字基础设施等领域。[#]

我国《网络安全法》赋予国家在此事项保障运行安全的强大权力或职责。对于关键信息基础设施,除了网络一般运行安全的保障职责之外,还具有以下多项重大保障权力:(1)实行重点保护。(第三十一条)(2)明确专门机构负责规划和监管。(第三十二条)(3)确保设施性能和保证安全技术措施同步。(第三十三条)(4)运营者应当履行特别安全保护义务。(第三十四条)(5)实行国家安全审查。(第三十五条)(6)采购应签订安全保密协议。(第三十六条)(7)实行境内个人信息和重要数据境内存储。(第三十七条)(8)实行运营者安全年检和报告。(第三八条)(9)国家网信部门还应统筹协调其他安全保护措施,包括抽查检测、定期组织进行网络安全应急演练、促进网络安全信息共享、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。(第三十九条)对于上述特殊权力,立法前后也产生不少争议,一种观点认为,这些保障措施特别是其中的审查机制、境内存储要求等过于严苛,没有被立法采纳。[$]

5. 网络信息安全保障

我国《网络安全法》第 4 章引入了多层次的信息安全概念,并在第 41 条至 50 条,确立了极有特色的网络信息安全保障制度。除了对于用户个人信息安全(立足个人隐私和身份信息利益的安全角度)的重点保障之外,还涉及对"禁止信息"(有害信息)的安全监管。后者立足的不再是个人信息利益保护,而是基于法律和行政法规上的社会安全、经济安全、国家安全的需要,实践中甚至可能超出一般意义的法律范围,扩及到一般的政治安全、文化安全、意识形态安全。[%] 比较起来,其他国家网络安全法关于网络信息安全的监管,没有采用广义的网络信息安全概念,而是以个人信息保护为重点,对于我们所谓的禁止信息问题,根据其涉及的网络言论、商业经营权等问题,认为通常只需要纳入一般法律框架处理即可,而不需要特别监管。

在比较法上,用户或个人信息安全监管,相对而言是网络安全管制中走得较快、立法上比较容易达成妥协的领域。在许多立法支持者看来,网络信息安全保障规制问题,是处理用户私的权利对网络商业私的权利

! 刘金瑞《我国网络关键基础设施立法的基本思路和制度建构》,《环球法律评论》2016 年第 5 期,第 116 页。

" 联邦政府和有关方面在涉及关键信息基础设施方面一直试图推动立法,赋予政府管制地位,但是遇到强大的反对力量。参见维基百科 "Cyber-security regulation",https://en.wikipedia.org/wiki/Cyber-security_regulation#endnote_kirby,最后访问时间:2017 年 2 月 17 日。

参见 DIS Directive,Art. 4 point(4), Annex II. 第 4(4) 条,附录 II。

$ 关于此处有关权力和义务规定的争议,特别是来自国外机构或企业在立法的批评,请参见《外媒:呼吁中国网络安全法重新考虑"争议条款"》,http://news.163.com/16/1108/15/C5C1UU7G000187V9.html,最后访问时间:2017 年 2 月 17 日;以及《中国网络安全法为何不受国外待见》,新华网,http://forum.home.news.cn/post/viewPost.do?id=140208241&pg=1&lan=en,最后访问时间:2017 年 2 月 17 日。但我国国内学者也有人认为,国外企业的批评似乎没有道理,刘金瑞《我国网络关键基础设施立法的基本思路和制度建构》,《环球法律评论》2016 年第 5 期,第 116 页。

% 王强春《网络传播与国家信息安全保障》,《上海政法学院学报》(法治论丛)2013 年第 1 期。

的关系,和其他问题涉及可能会导致武断赋予政府权力不太一样。欧盟较早就制定了《个人数据保护指令》。[!] 以对网络安全立法比较谨慎的美国为例,关于网络信息安全这一块除了得到许多州法支持之外[",]也比较早获得一些联邦立法支持。欧盟关于个人信息安全保护措施比较明确,甚至建立了一些新型权利,比如可携带权、遗忘权等;但是在美国,有关联邦立法还是很有阻力,难以明确确立施加所有互联网企业的相应保障义务,目前只是笼统地规定了有关特殊机构(医疗、金融、联邦机构等)需要承担信息安全的保护义务[#],且缺少具体措施和标准,只要求达到所谓"合理水平"[$],实践中用户信息保护目前主要靠各州法律、判例和企业自律。[%]

我国《网络安全法》第四章,总体上可以区分两项监管事项。第一部分是用户信息安全保障,第二部分是禁止信息管制保障。

(1)用户信息安全保障。

这一部分我国以保障用户信息安全为重心,通过设定网络运营者若干信息安全保障义务、用户享有特别保障权利、禁止窃取等非法针对信息活动以及对接触用户信息的管理机构设置特别保障义务多个方面建立保障体系。

首先,规定网络运营者负有多项信息安全保障义务。包括:(1)严格保密信息和健全信息保护制度。[&](2)合规收集和使用信息。[']即应当遵循合法、正当、必要、公开、明示、用户同意的原则和要求,禁止超出服务范围收集、违反法律或者约定收集或使用,应当依照法律和约定处理其保存的信息。(3)妥当保全信息。[(]包括:禁止泄露、篡改、毁损收集的个人信息;禁止未经同意向他人提供收集信息(应当采取技术等必要措施确保信息保全,发生泄露、毁损、丢失的信息安全事件应当立即补救并告知用户和向主管机构报告。不过,前两项保全规定不是绝对的,考虑到数据产业的发展,立法为合理加工数据和合法数据交易留下余地,第 42 条第 1 款最后一句立法表述为"但是,经过处理无法识别特定个人且不能复原的除外"。

其次,规定用户享有多项特殊保障权利,包括删除和更正权。[)] 对于运营者违法或者违约的收集、使用可以要求删除信息;发现运营者收集、存储信息错误可以要求更正。应当注意到的是,这里的删除权与欧盟指令的遗忘权有相似之处,但并不相同,有条件的即以运营者违法或违约为前提。此外,我们没有规定欧盟和其他国家的可携权。

再次,禁止针对信息的非法活动。[†] 包括:任何组织不得以窃取或其他非法方式获得信息;不得非法出售或提供个人信息。这一规定在《网络安全法》属于不完整规定,其本身在法律责任部分并没有对应的特别责任规定,因此需要依据法律责任部分的第 74 条[*]等转接规定,作为确立一种法定义务的基础规范而链接其他法律的适用。

最后,设定管理机构和人员的尽职管理的保障义务。[‡] 监管机构和人员对于知悉的信息严格保密,不得泄露、出售或非法提供。

! 欧盟最早在 1995 年 10 月 24 日通过了《个人数据保护指令》(EU Data Protection Directive)。2016 年修订通过了一部新的《一般数据保条例》,取代原来的指令,将于 2018 年 5 月 25 日正式生效。

" 参见"Notice of security breach-civil code sections 1798.29 and 1798.82 - 1798.84"(2003),updated: 2005 - 11 - 23; Rasmussen, M., & Brown, A. "California Law Establishes Duty of Care for Information Security"(2004), updated: 2005 - 11 - 31.

参见 Heiman, B. J. "Cybersecurity regulation is here", RSA security conference(2003), Washington, D. C. updated: 2005 - 11 - 17.

$ 参见 Kirby, C. "Forum focuses on cybersecurity", updated: 2003 - 12 - 04, San Francisco Chronicle; Lemos, R. "Bush unveils final cyber-security plan"(2003), updated: 2005 - 12 - 04.

% 以上关于美国联邦信息安全保护立法资料的介绍,出自维基百科: Cyber-security regulation, https://en.wikipedia.org/wiki/Cyber-security_regulation#endnote_rasmussen, 最后访问时间: 2017 年 2 月 17 3 !&] P :

&

'

(

)

†

*

‡

(2) 禁止信息管制保障。

《网络安全法》从第四十六条到第五十条建立了独特的禁止信息管制制度,发布涉及违法犯罪活动的信息或者其他法律和行政法规禁止的信息的,受这一制度管制。

首先,禁止发布涉及犯罪或者违法的有害信息,包括直接行为,也包括间接行为。第四十六条规定禁止设立用于违法犯罪活动的网站、通讯组群,禁止利用网络发布涉及违法犯罪活动的信息。[!] 第四十八条规定,禁止利用应用软件或设置恶意程序发送禁止信息。["]

其次,规定网络经营者负有监管有害信息的义务。第四十七条规定网络运营者对有害信息有加强管理义务,发现情况应当立即停止传输,采取措施防止扩散,并且保存记录并报告。[#] 第四十九条规定网络运营者应当设置网络信息安全投诉、举报机制(包括建立制度公布信息、及时受理和处理等要求,这既适用于用户信息保护,也适用于有害信息管制;同时应当配合有关部门的监督检查。[$]

共利益,基于处置突发社会安全事件的需要,可以在特定区域对网络通讯采取限制等临时措施,这相当于一种准司法权力。[!]

四、我国网络安全管制实施的限定因素

《网络安全法》推崇国家管制功能,建立了一个强大的国家监管体系,通过具体制度设计赋予了国家广泛的事项管制力,要求较高且普遍刚性。["] 然而,对于这样一部强监管法律,从合理而有效实施的角度而言,必须特别注意其实施中的边界问题,特别是其中国家管制权力的界限问题。

(一) 网络管制规范的目的和体系限定

任何法律从其适用基本原理出发,都需要通过目的和体系解释加以适用,管制规范就其特性来说更需要如此。《网络安全法》确立的管制规范,从法律体系上说,应当受到《网络安全法》之外的广义法律目的和体系的限定,也应当受到《网络安全法》本身目的和体系的限定。对于《网络安全法》之外的限定,比如宪法作为其上位法的优位性,其与刑法、民法、诉讼法等基本法律的关系,与一般行政法和其他像《国家安全法》等具体行政法的关系等等,非常复杂,限于篇幅,在此不展开解释。这里只简单阐述《网络安全法》本身的目的和体系限定要求。

1.《网络安全法》的目的限定

《网络安全法》第二条规定"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。"可见,《网络安全法》顾名思义,从规范目的和立法定位角度来说,是一部专门明确以网络安全为规范对象的特别法,旨在通过确立网络安全管制以达成网络安全。所以,它从目的上说,直接服务于保障网络安全,该法中的那些规范特别是管制规范,应当限于这个目的事项本身而加以适用。《网络安全法》管制规范的实施,无论是其机构管制权力或职责,还是关于运营者的法定义务规定,还是包括用户在内的其他主体的对应义务或特殊保障权利,首先应该合乎处于法律体系最高位置的目的,目的构成一部法律的基本限定。此外,具体规范之间发生冲突时也存在适用中基于目的的利益衡量问题。

《网络安全法》的目的限定性,提醒我们应当严格把握该法的适用范围,即应该严格限于网络安全事项本身。不能离开目的限定,转而简单从规范内容或效果出发,对网络安全规制的对象加以曲解,否则很容易导致过宽理解网络安全规制范围。如果从规范内容来看,《网络安全法》范围涉及网络主体、管理机制、行为方式、保护范围、义务要求、责任、人才培养等,如果从规范的效果来看,既有助于维护网络秩序,也维护了国家、社会、个人以及法人和其他组织的合法利益。[#] 但是,对于《网络安全法》适用范围的理解,如果从目的出发,结合第一条目的条款,我们应该认识到,网络安全规制的对象是严格意义的网络安全事项,而不能理解为一般的网络事项,否则会使得本法成为泛泛的网络管理法而不是的网络安全法。由此限定,《网络安全法》设定的一切管制权力和一切受管制义务,其行使指向必须结合本法为应对网络安全本身的事项范围而加以严格解释。管理机构不得脱离网络安全规制的直接必要目的和规制范围,简单以保护国家、社会或他人权利的需要为借口而行使该法赋予其的权力,受规制的网络运营者、服务者和用户等,也无须基于对一般法律秩序或者他人权利尊重和保护本身而便需要承担此中的强力管制义务和责任。应当把握,《网络安全法》虽然也能够间接实现有利于有关法律利益保护的效果,但是它不是直接追求保护这些法律利益本身的,否则会导致网络安全法适用的泛化理解。[$]

! 参见《网络安全法》第五十八条。

" 《网络安全法》在第六章有针对性地对管理机构执行管制权力、经营者履行保障义务规定了警告、罚款、责令补救等行政处罚的法律责任,作为具体的责任保障,使这些管制规范具有更明显的刚性。

参见刘黎明、辛力《〈网络安全法(草案) 〉评析》,《上海政法学院学报(法治论丛) 》2016 年第 5 期。

$ 我国《网络安全法》第一条注意到了网络安全和法律利益的关系,但其表述本身却容易引起适用范围的歧义。该条规定"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。"可见,表述上将作为直接适用对象的网络安全与作为适用而取得的法律效果一体化并列,如此不免模糊了法律适用范围的限定性。

2.《网络安全法》的体系限定

《网络安全法》采取了总则加具体章节的结构,除了第一条和第二条(目的条款和调整对象条款)之外,第三条以下均为原则表述或概括性规定。原则在制定法的体系之中,是用来概括或构筑法律基本价值的,[!] 其本身不能直接援引作为管制授权基础,但是应当作为具体规范包括管制规范的体系限定基础。即原则构成法律体系中的内在价值体系,对于法律外在体系具有限制功能。["]

《网络安全法》的所有原则条款中,第三条规定了网络安全与信息化发展并重的原则,网络安全和信息化发展是本法平行追求的价值,二者绝对不能偏废。[#] 这一原则作为彰显价值的条款居于诸原则条款的突出位置,最具有优先性;其他多数是管制抽象授权条款(第四条到第八条

网络最初最小化设计架构通过在应用层的不断锲入,成为一种为各种特殊应用目的控制的架构。[!] 正是因为如此,我们看到许多网络政治家和产业代表根本不信任通过简单推行政府管制就可以产生管制作用,从网络是一种特殊架构的角度,他们更加相信只有那些写出或者采用锲入代码的网络机构本身心甘情愿配合网络安全才能真正达成网络安全保障的效果,所以设计有效的网络安全治理体系不能忽视网络技术架构的存在,否则规则不仅无益而且还导致不必要的负担。["] 比如,美国政府克林顿时期曾经就解密晶片使用加密技术同时应当为政府预留后门问题,最早打算通过直接管制的方式达成,但是在遇到产业界和理论界广泛质疑之后,明智地转向更加间接也更具有优势的市场策略方案。[#] 可见,从网络的技术组织架构特点和管制执行的效率角度来看,网络管制很多情况下并不适宜直接化,而是需要更多与控制网络技术架构的机构合作。

我国《网络安全法》注意到了网络空间的技术架构和组织架构的复杂性,在一些方面引入了政府与网络运营者合作治理的思想,也试图通过一些激励机制的方式来鼓励、引导网络运营者重视网络安全。例如,在关键信息基础设施安全保障上,就规定要"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",这就是一种很好的符合网络技术架构特点的设计,也是全球普遍的做法。比如,美国《网络安全　　在的重点就是对信息安全,将[illegible]很多的问题立法明确下来。

但是,我国《网络安全法》对于网络空间技术架构[illegible]面甚至没有顾及,总体上比较依赖国家单方面的管制力,管制直接且比较刚性,因此在实践中可以中必定会遭遇与有关网络技术架构、互联网商业利益协调的复杂性和困难性。这种情况,将来应进一步完善。例如,可以[illegible]引入责任减轻等激励机制来支持企业自觉加入安全信息共享同样必要的,也应当在接下来特殊环境,以复杂实践要求的

我国刚刚出台的《网络安全法》肩负美好愿望,旨在有效应对当今复杂多变的网络安全问题,进而匡扶网络空间。但是,"一法出,天下平"的理想,不是简单就能够实现的,而是需要我们在法律实施上真正地有所作为。

这部法律得到有效实施的前提,在于我们能否很好地理解其确立的内在基础所在以及有关网络安全管制架构的内涵和界限。本文通过研究认为,我国《网络安全法》是一部强监管的法律,在当今世界的网络安全专门立法中可谓独树一帜。首先,它建立在一个更加多层次网络安全管理的概念基础上,这就使得它的面向较多,管制内容丰富。其次,也是比较重要的,它以一种强化国家管制力的方式实现治理网络安全的愿景,确立了一个广泛而刚性的国家管制架构。所以,我们在实践中应当持有一种格外审慎,深刻把握网络安全管制的正当化基础和运行界限,特别是要注意结合目的体系、行政权本质以及技术架构等因素,对相关管制规范的实施做出必要的限定解释。笔者期待,上述研究对于我国《网络安全法》接下来的实施能具有一定的指导价值。

[责任编辑　李晶晶　责任校对　王治国]

! [美] 劳伦斯·雷席格著,刘静怡译《网络自由与法律》,台北: 台湾商周出版社 2002 年版,第 99 页以下,"第四章控制的结构"。劳伦斯·雷席格深刻阐述了网络的基础是代码的思想,由此提出网络管制仅仅依靠政府的直接管制方式是不可能有效的,需要政府和可以操纵网空间特殊架构即代码的网络机构或企业进行合作,应当透过控制代码而进行管制,或者根据代码不同而进行不同的管制区分(如公开代码和封闭代码对政府行为作用影响就差别很大) 。

" 参见 Brendan Sasso, "After defeat of Senate cybersecurity bill, Obama weighs executive-order option", updated: 2012 - 08 - 04, The Hill, Accessed, updated: 2012 - 08 - 20.

参见 Stewart A., "Baker and Paul R. Hurst, The Limits of Trust: Cryptography, Governments, and Electronic Commerce, Kluwer Law International", 1 Edition updated: 1998 - 08 - 01, pp. 15 - 22.

$ 参见美国《网络安全法》第一编"网络信息共享"。