「국제법무」 제9집 제2호, 2017. 11. 30.
제주대학교 법과정책연구원

中国《网络安全法》开启中国网络安全新时代

China's Cybersecurity Law commences a New Era of Cybersecurity in China

마오페이*
Miao, Fei

目 次

국문초록

인터넷 시대가 되면서 인터넷은 우리의 정치와 경제, 사회 생활의 각 방면에 깊숙이 파고들어 세상을 변화시키고 있다. 사이버 공간의 발전은 우리에게 편리함을 안겨 주는 한편, 사이버 범죄를 야기하여 시시각각 사이버 안보를 위협하고 있다.

중국 정부는 이와 같은 사회적 변화와 새로운 위협에 대응하기 위해 "중화인민공화국네트워크안전법"(이하 "네트워크안전법")을 2016년 11월 7일 제정하여 2017년 6월 1일부터 시행하고 있다.

중국 정부는 네트워크안전법의 제정 목적에서 사이버 주권과 국가안보, 사회 공공이익을 수호하기 위해 네트워크보안을 강화함을 밝히면서 중국의 사이버안보

논문접수일 : 2017. 09. 30.
심사완료일 : 2017. 10. 19.
게재확정일 : 2017. 10. 20.
* 김·장 법률사무소, 중국변호사

에 대한 관심과 전략방향을 잘 보여주고 있다. 동시에 중국 네트워크 보안체계의 종합적인 정비를 목표로 법안에 네트워크 보안전략의 제정, 안전등급 보호제도의 시행, 네트워크 핵심 장비 및 보안 전용 제품에 대한 안전 인증 및 검사제도 시행 그리고 핵심 정보인프라 지정 보호를 위한 방법을 자세히 규정하고 있다. 또한 법안에 자국민 개인정보를 처리하는 기업이 수집한 데이터를 중국 영토 내 보관을 원칙으로, 비즈니스 목적의 해외저장 데이터는 중국 정부의 승인을 필요하도록 규정함으로써 자국데이터에 대한 통제의도를 명확히 밝히고 있다.

이 법의 내용은 중국 내 인터넷서비스사업자뿐만 아니라 수많은 외국계 기업에도 미칠 가능성이 매우 크다는 점에서 주목을 받고 있다.

본 논문은 네트워크안전법의 입법 배경 및 제정 과정, 주요 조항과 부대 법의 입법 목적 등의 해석을 통해 동법의 입법 목적 및 규제 내용에 대한 이해를 돕기 위해 작성되었다.

주제어 : 사이버 보안, 네트워크안전법, 정보 보호, 정보 보안, 핵심정보 인프라, 사이버 범죄, 국가안보

绪论

进入21世纪以来，网络空间飞速发展，世界开始进入网络时代，网络安全也迎来了严峻的挑战。在这样的大背景下，包括中国在内的世界各国都在加紧出台规制网络空间的法律法规，比如美国的《2015年网络安全法案》、欧盟的《通用数据保护条例》和《网络信息安全指令》以及德国的《IT安全法》等等。

2016年11月7日，第十二届全国人大常委会第二十四次会议以154票赞成、1票弃权表决通过了《中华人民共和国网络安全法》（以下简称“《网络安全法》”），于2017年6月1日起开始施行。《网络安全法》不仅是国家安全法律制度体系中的一部重要法律，更是中国网络安全领域的第一部综合性及基础性的法律。

本文将对《网络安全法》进行全面解读，包括《网络安全法》的出台背景及制定过程、主要条款和配套规定等。

一、《网络安全法》的出台背景及制定过程

(一)《网络安全法》的出台背景

1. 网络犯罪严重威胁网络安全

根据有着“互联网女皇”之称的华尔街证券分析师玛丽·米克尔于2017年6月1日在美国Code大会上发布了的《2017年互联网趋势报告》显示，目前全球互联网用户为34亿[1]。而根据中国互联网信息中心发布的《第40次中国互联网发展状况统计报告》，截至2017年6月，中国网民规模达到7.51亿，互联网普及率为54.3%[2]。从上述数据可以看出，全球的网民人数已经接近达到全球人口的二分之一，而中国网民人数也已超过了全球网民总人数的五分之一。

然而，随时网络信息时代的发展及网民人数的大幅增长，网络安全问题开始引起了各国的关注。2016年，国家互联网应急中心共接收境内外报道的网络安全事件125,660起，在接收的网络安全事件中，排名前三位的分别是网页仿冒事件（占42.3%）、漏洞事件（24.6%）和恶意程序事件（12.0%）[3]。上述网络安全事件发生的原因除了相关技术发展的不成熟，还有相关法律法律和监管政策的不完善。因此，只有完善网络安全立法，确保网络空间的妥善监管，才能保障网络空间安全健康地发展。

2. 《网络安全法》出台前打击网络犯罪的法律依据

在《网络安全法》出台以前，打击网络犯罪主要依据《中华人民共和国刑法》（以下简称“《刑法》”）、中国最高人民法院、最高人民检察院（以下简称“两

1) 玛丽·米克尔，《2017年互联网趋势报告》，2017年，第5页。
2) 中国互联网信息中心，《第40次中国互联网发展状况统计报告》，2017年，第13页。
3) 国家计算机网络应急技术处理协调中心，《2016年中国互联网网络安全报告》，人民邮电出版社，2016年，第33页。

高”）关于网络犯罪、网络案件的司法解释以及有关网络安全和信息保护的法律规范，如《刑法》第六章第一节中规定的非法侵入计算机信息系统罪、破坏计算机系统罪、非法利用信息网络罪等，及两高于2011年颁布的《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》及2013年颁布的《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》，以及全国人大常委会于2000年颁布的《关于维护互联网安全的决定》和2014年颁布的《关于加强网络信息保护的决定》。然而，随着网络安全事件和网络犯罪的频发，上述法律法规及司法解释不足以为打击网络犯罪提供充分的法律依据。因此，中国亟需加强惩治网络犯罪、保护网络安全的相关立法。

3. 制定《网络安全法》的必要性

进入网络时代以来，网络不可避免地已经融入到了政治、经济以及社会生活的各个方面，网络空间的发展时刻都在改变和影响着我们的生活。诚然，网络给我们的生活带来了无限的便利，网络也必然会在未来作为基础设施而存在，但同时，开放共享的网络环境也使我们时刻处在危险之中。中国网络治理起步较早，1994年国务院发布《计算机信息系统安全保护条例》，开了中国网络治理的先河，此后国家先后出台了近200部涉及互联网的法律法规和规范性文件，但这一治理系统显然存在着一定的瑕疵[4]。随着网络安全问题的日益凸显，以及网络犯罪行为的日益增长，为了保障网络安全，维护社会公共利益，保护公民、法人等的合法权益，在既有法律法规的基础上制定一部基础性原则性的网络安全相关的法律则势在必行。

4. 《网络安全法》的出台顺应了网络法制化趋势

《网络安全法》的出台顺应了网络法制化的趋势，是落实国家总体安全观的重要举措。自十八大以来，党中央从总体国家安全观出发，对加强网络安全工作作出了重要部署，对加强网络安全法制建设提出了明确要求。2014年2月27日，国

4) 庹继光，“《网络安全法》的治理思路辨析”，【新闻与法治】，2017年，第40页。

家主席、中央网络安全和信息化领导小组组长习近平曾指出："没有网络安全就没有国家安全"。2015年7月1日，《中华人民共和国国家安全法》（以下简称"《国安法》"）出台并生效。《国安法》首次明确提出，中国将"维护国家网络空间主权、安全和发展利益"，具体如下：

"国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。（第二十五条）"

相比《国安法》就网络安全作出的原则性规定，2017年6月1日生效的《网络安全法》的通过不仅是顺应中国网络安全工作的新形势，落实中央决策部署，保障网络安全和发展利益的重大举措，更符合了维护网络安全及国家广大人民群众切身利益的客观需要。同时，由于近年来中国积极参与了互联网国际规则的制定，虽然中国的竞争力和话语权逐渐增强，然而仍与发达国家有一定差距，为了增加中国的国际竞争力，《网络安全法》的制定和出台亦是中国参与互联网国际竞争和国际治理的必然选择。

（二）《网络安全法》的制定过程

2013年10月，制定网络安全法列入十二届全国人大常委会立法规划；2014年上半年，法工委掌握各方面的立法需求；2014年5月，确定总体思路，起草大纲；6月，拟定主要制度初步方案；10月，完成草案初稿[5]。

2015年初，形成了草案征求意见稿；2015年6月26日，全国人大常委会委员长会议将《网络安全法（草案）》提请十二届全国人大常委会第十五次会议进行初次审议，十二届全国人大常委会第十五次会议对《网络安全法（草案）》进行了分组审议。

2015年7月6日至2015年8月5日期间，《网络安全法（草案）》向社会公开征求

5）宋燕妮，"《网络安全法》开启我国网络立法新进程"，【信息安全研究】第三卷，2017年，第569页。

意见，并根据全国人大常委会组成人员和各方面的反馈意见，对草案进行了修改，形成了《网络安全法（草案）》二次审议稿。

2016年6月28日，十二届全国人大常委会第二十一次会议对《网络安全法（草案）》二次审议稿进行了分组审议。

2016年7月5日至2016年8月4日，《网络安全法（草案）》二次审议稿正式在中国人大网公布，并向社会公开征求意见。

2016年10月31日，十二届全国人大常委会第二十四次会议对《网络安全法（草案）》进行了第三次审议。

2016年11月7日，全国人大常委会以154票赞成、1票弃权的表决结果通过了《网络安全法》。

二、《网络安全法》的重点条款及解读

《网络安全法》共计有七章七十九条规定，具体内容涉及其调整范围、网络运行安全、关键信息基础设施安全、个人信息保护、监测预警及应急处理、法律责任等，明确了多方面的网络安全要求，包括维护国家网络空间主权、保护关键信息基础设施与重要数据、保护个人隐私信息、明确各方网络安全义务等。本文将对《网络安全法》的重点条款作出解读，具体如下。

(一)《网络安全法》确立了三大基本原则

1. 网络空间主权原则

《网络安全法》在开篇第一条就明确了立法目的，即：

“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。（第一条）”

网络空间并非法外之地，网络空间主权是一国国家主权在网络空间的自然延伸

和表现。《联合国宪章》确立的主权平等原则为当代国际关系的基本准则，而该准则同时也应该适用于网络空间，因此，各国有权自主选择网络发展道路和网络治理模式。

《网络安全法》同时确定了其管辖范围，即：

“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。（第二条）”

该条对管辖范围的规定体现了中国对网络空间主权的最高管辖权。

2. 网络安全与信息化发展并重原则

习近平总书记在2016年4月19日主持召开的网络安全和信息化工作座谈会上指出，*“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。网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施”*。《网络安全法》第三条也明确规定，国家坚持网络安全与信息化并重，遵循积极利用、科学发展、依法管理、确保安全的方针；既要推进网络基础设施建设，鼓励网络技术创新和应用，又要建立健全网络安全保障体系，提高网络安全保护能力。

3. 共同治理原则

网络空间安全并非只是国家和政府的责任，网络空间安全需要政府、企业、社会组织、技术社群和公民等网络利益相关者等全社会的共同参与来共同守护。《网络安全法》坚持共同治理原则，明确了政府部门、网络建设者、网络运营者、网络服务提供者、网络行业相关组织、高等院校、职业学校、社会公众等各自的角色及义务。

（二）网络运营者及其安全保护义务

2017年6月1日起正式施行的《网络安全法》明确确定了“网络运营者”的概念，

并且在本法中“网络运营者”一共出现了31次，且有14个条文规定了“网络运营者”的安全保护义务。下面将分别讨论网络运营者的定义及其安全保护义务。

1. 网络运营者的定义

《网络安全法》第七十六条第3款规定*“网络运营者，是指网络的所有者、管理者和网络服务提供者”*。从网络运营者的定义来看，“网络运营者”包含三类主体，即网络的所有者、网络的管理者以及网络服务提供者，但是《网络安全法》却并未对网络的所有者、网络的管理者以及网络服务提供者进行进一步的定义，这就导致了“网络运营者”的表述涉及的范围非常广泛， 通过网络提供服务、开展业务活动的企业及机构，都可能被视为“网络运营者”[6]。但是，实际上“网络运营者”的定义在《网络安全法（草案）》中被规定地更加明确：

《网络安全法（草案）》第六十五条规定*“网络运营者，是指网络的所有者、管理者以及利用他人所有或者管理的网络提供相关服务的网络服务提供者，包括基础电信运营者、网络信息服务提供者、重要信息系统运营者等。”*。

对比上述规定的变化来看，立法者之所以修改了《网络安全法（草案）》中“网络运营者”的定义，使得这一定义更加开放及宽泛，必定是考虑到了由于网络空间的飞速发展，如果对“网络运营者”进行带有框架的确定的定义，则为“网络运营者”设定了局限，使其无法顺应网络空间的高速发展，从而导致《网络安全法》的滞后，因此只规定“网络运营者”的内涵而对其外延采取开放的描述方式则是一种更明智的选择。

2. 网络运营者的安全保护义务

在《网络安全法》实施以前，网络运营者的安全保护义务主要由《侵权责任法》进行规定，而在上述《侵权责任法》中，安全保护义务的主体仅限于“网络服务提供者”，即“网络运营者”包含的三类主体之一，具体的安全保护义务也仅限于事后止损义务，具体如下：

6) 毕马威中国，《网络安全法》概览，2017年，第9页。

“网络用户利用网络服务实施侵权行为的，被侵权人有权通知网络服务提供者采取删除、屏蔽、断开链接等必要措施。网络服务提供者接到通知后未及时采取必要措施的，对损害的扩大部分与该网络用户承担连带责任。（第三十六条）”

从上述规定可以看出，《侵权责任法》规定的对网络服务提供者的安全保护义务主要是关于网络服务提供者在经营过程中的合理注意义务，并不能据此有效解决并管理网络安全问题。而《网络安全法》的实施，将作为网络安全领域的基本法，有效解决网络安全问题。

《网络安全法》对网络运营者的安全保护义务作出了一般性的规定：

“国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。（第二十一条）”

上述条文规定了具体的网络运营者的安全保护义务，包括确定网络安全负责人义务，技术管理保障义务，数据安全义务及兜底条款。该条虽未能涵盖所有网络运营者的安全保护义务，但是设定了兜底条款，为未来根据发展增加新的义务提供出口，同时还可以避免技术进步对法律稳定性产生的影响。

《网络安全法》的第二十一条对网络运营者安全保护义务作出的一般性规定，是《网络安全法》中关于网络安全保护义务的所有规定的最高原则及其他条款的基础。除此之外，《网络安全法》还在在第四十一条、第四十二条、第四十三条、第四十四条、第四十五条规定了网络运营者的个人信息保护义务，在第四十六条、第四十七条、第四十八条规定了网络运营者的内容管理义务，以此作为对第二十一条的进一步细化和补充，使得网络运营者安全保护义务更加完善和健全。

(三) 关键信息基础设施的运行安全

《网络安全法》首次提出了“关键信息基础设施”的概念，并设专门一节来规定关键信息基础设施的范围、保护机制、国家安全审查等内容。

1. 关键信息基础设施的定义

根据《网络安全法》第三十一条的规定，关键信息基础设施是指一旦遭到破坏、丧失功能或数据泄露，将对中国国家安全、国计民生、公共利益造成重大危害的重要网络设施和系统，包括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。《网络安全法》并未对关键信息基础设施的具体范围进行确定，而是规定了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。目前，有关关键信息基础设施的配套法规，如《关键信息基础设施安全保护条例》、《信息安全技术关键信息基础设施安全保障评价指标体系》、《关键信息基础设施识别指南》等一系列法规正在制定之中。因此，在配套法律法规出台之前，按照目前的定义表述，关键信息基础设施的潜在覆盖范围非常广泛，只能待法律进一步进行明确。

2. 关键信息基础设施运营者的义务

关键信息基础设施运营者除了需要履行《网络安全法》第二十一条规定的按照网络安全等级保护制度的要求需履行的安全保护义务以外，还需要履行如下安全保护义务：

“（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

（三）对重要系统和数据库进行容灾备份；

（四）制定网络安全事件应急预案，并定期进行演练；

（五）法律、行政法规规定的其他义务。（第三十四条）”

第三十四条规定的关键信息基础设施的安全保护义务是在第二十一条规定的网络运营者安全保护义务的基础之上的重点保护义务，相比较于网络运营者的安全保护义务，关键信息基础设施运营者的义务更加严格。另外，第三十八条同时要求关键信息基础设施运营者每年至少自行或委托专业机构进行一次安全风险检测评估。类似的规定也体现在了《信息安全等级保护管理办法》中，该办法要求安全等级为第三级的计算机信息系统的运营者每年至少进行一次安全自查以及委托专业机构进行一次安全等级测评。

3. 国家安全审查

关键基础设施作为大数据赖以存续的载体，如若遭遇威胁，数据安全将面临重大挑战[7]。为防止关键信息基础设施因使用的产品和服务存在安全缺陷或者其他隐患而受到攻击、破坏，或者其存储、处理的数据资源被窃取、泄露，危害国家安全[8]，《网络安全法》规定"*关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查*"[9]。该等规定遵循并落实了《国安法》确立的国家安全审查制度，具体为：

"国家建立国家安全审查和监管的制度和机制，对影响或者可能影响国家安全的外商投资、特定物项和关键技术、网络信息技术产品和服务、涉及国家安全事项的建设项目，以及其他重大事项和活动，进行国家安全审查，有效预防和化解国家安全风险。（第五十九条）"

除了在影响国家安全情况下的国家安全审查，关键信息基础设施运营者采购网络产品和服务，还应当按照规定与提供者签订安全保密协议[10]。

---

7) 齐爱民，"论大数据时代数据安全法律综合保护的完善-以《网络安全法》为视角"，【东北师大学报（哲学社会科学版）】，2017年，第111页。

8) 宋燕妮，"《网络安全法》开启我国网络立法新进程"，【信息安全研究】第三卷，2017年，第569页。

9)《网络安全法》第三十五条。

10) 《网络安全法》第三十六条。

4. 关键信息基础设施重要数据的跨境流动

随着网络时代的发展，包含大量的个人信息以及涉及国家安全、经济安全的重要数据的跨境流动也在不断增加，同时给数据安全带来威胁。受棱镜门事件影响，数据本地化（Data Localization）风潮席卷全球，俄罗斯、德国、巴西、韩国、印度等国家纷纷出台相关政策或立法，限制数据跨境流动[11]。在《网络安全法》未出台之前，中国仅在一些特定行业立法中有所涉及，例如《征信业管理条例》第二十四条规定，征信机构对在中国境内所采集信息的任何处理以及存储均须在中国境内进行，如若向境外提供信息，须遵守中国相关规定；又如《地图管理条例》第三十四条规定，互联网地图服务单位存放地图数据的服务器必须设在中国境内，并要制定互联网地图数据安全管理制度和保障措施[12]。《网络安全法》的出台明确了数据本地化的基本原则，即关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储，因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估[13]。

(四) 用户个人信息保护制度

用户信息保护制度也并非首次出现在中国的法律法规中。在《网络安全法》颁布之前，已经有多部法律法规或部门规章从不同层级及针对不同业务模式，对用户个人信息的保护作出了相应的规定[14]。具体的规定包括但不限于《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》、《中华人民共和国消费者权益保护法》、《电信和互联网用户个人信息保护规定》和《规范互联网信息服务市场秩序若干规定》[15]。此次《网络安全法》以国家基本法律的形式 采用专章

11) 齐爱民，“论大数据时代数据安全法律综合保护的完善-以《网络安全法》为视角”，【东北师大学报（哲学社会科学版）】，2017年，第112页。

12) 同上。

13)《网络安全法》第三十七条。

14) 刘斯佳，《中华人民共和国网络安全法》之关键信息基础设施重点保护制度要点解读，环球法律专递，2016年，第2页。

对网络信息安全作出一般规定，确立网络信息安全的总体目标和基本原则，明确网络运营者收集、使用个人信息的一般规范和罚则；建立网络信息保密制度，保护网络主体的隐私权；建立行政机关对网络信息安全的监管程序和制度，规定对网络信息安全犯罪的惩治和打击；以及规定具体的诉讼救济程序等16)。

《网络安全法》对于用户个人信息的保护主要分为五大方面。

其一，通过第四十一条就个人信息的采集和使用，明确了合法、正当和必要的三原则，提出了需要信息被收集者同意的要求。此外，第四十一条明确规定了*“网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息”*。

其二，通过第四十二条确立了对于泄露、损毁、丢失个人信息的补救措施和告知报告制度，其目的主要是约束了网站等网络经营者的行为。

其三，通过第四十三条赋予了公民个人信息删除权和更正权。具体来讲，公民个人主要有两个层面的权利，第一个权利即个人在发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息，第二个权利即个人在发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。

其四，通过第四十四条及第四十五条建立了保密制度，即任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息，依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

其五，是通过第四十六条及第四十七条确立了网络使用的行为责任及管理责任，即任何个人和组织应当对其使用网络的行为负责，网络运营者应当加强对其用户发布的信息的管理，发现法律、行政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，防止信息扩散，保存有关记录，并向有关主管部门报告。

---

15) 同上。

16) 陈璐，“论《网络安全法》对个人信息刑法保护的新启示-以两高最新司法解释为视角”，【法治研究】，2017年，第87页。

(五) 法律责任

《网络安全法》在第六章“法律责任”中对网络运营者等主体的法律义务和责任做了全面规定。其中，网络安全保护和监督管理的负责部门包括国家网信部门、国务院电信主管部门、公安部门及其他有关机关，法律责任承担主体包括网络运营者、关键基础设施运营者、网络产品服务提供者、信息软件发布服务提供者等。《网络安全法》的“法律责任”篇章与“网络运行安全”、“网络信息安全”、“监测预警与应急处置”等章节相互呼应，明确、细化了上述主体的法律义务，包括守法义务，遵守社会公德、商业道德义务，诚实信用义务，网络安全保护义务，接受监督义务等。而具体的处罚措施则根据具体违法行为的不同分为罚款、治安管理处罚民事责任以及刑事责任。

总体来看，《网络安全法》在“法律责任”一章中提高了违法行为的处罚标准，加大了处罚力度，有利于保障《网络安全法》的实施。

三、《网络安全法》的配套规定

为了保障《网络安全法》中规定的各项制度的有效实施，自《网络安全法》施行以来，国家互联网信息办公室等监管部门正在积极推进相关配套法规的研究与制定工作，且部分正在向社会征求意见，部分已经正式出台并生效。《网络安全法》及其配套法律法规和规范性文件汇总目录 （截至2017年9月16日）如下：

《网络安全法》及其配套法律法规和规范性文件汇总目录[17]

截止时间：2017年9月16日

序号	文件名称	发布机构	生效时间	法律状态
《网络安全法》及其配套规章和规范性文件				
基本法律和国家战略				
2	《国家安全法》	全国人大常委会	2015-7-1	现行有效
3	《网络安全法》	全国人大常委会	2017-6-1	现行有效

17) 陈际红、包达，《网络安全法》相关配套法律法规和规范性文件梳理，中伦观点，2017年。

3	《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》	全国人大常委会	2012-12-28	现行有效
4	《国家网络空间安全战略》	国家互联网信息办公室	2016-12-27	现行有效
5	《网络空间国际合作战略》	外交部和国家互联网信息办公室	2017-3-1	现行有效
互联网信息内容管理制度				
6	《互联网信息服务管理办法（2011修订）》	国务院	2011-1-8	现行有效
7	《互联网信息内容管理行政执法程序规定》	国家互联网信息办公室	2017-6-1	现行有效
8	《互联新闻信息服务管理规定》	国家互联网信息办公室	2017-6-1	现行有效
9	《互联网新闻信息服务许可管理实施细则》	国家互联网信息办公室	2017-6-1	现行有效
10	《互联网跟帖评论服务管理规定》	国家互联网信息办公室	2017-10-1	已发布，未生效
11	《互联网论坛社区服务管理规定》	国家互联网信息办公室	2017-10-1	已发布，未生效
12	《互联网群组信息服务管理规定》	国家互联网信息办公室	2017-10-8	已发布，未生效
13	《互联网用户公众账号信息服务管理规定》	国家互联网信息办公室	2017-10-8	已发布，未生效
网络安全等级保护制度				
14	《信息安全技术 网络安全等级保护实施指南（征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效
15	《信息安全技术 网络安全等级保护测评过程指南（征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效
16	《信息安全技术 网络安全等级保护测试评估技术指南（征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效
17	《信息安全技术 网络安全等级保护基本要求（第1-5部分）（征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效
18	《信息安全技术 网络安全等级保护设计技术要求（第1-5部分）（征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效
19	《信息安全技术 网络安全等级保护测评要求（第1-5部分）（征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效
关键信息基础设施安全保护制度				
20	《关键信息基础设施安全保护条例（征求意见稿）》	国家互联网信息办公室	N/A	正式版未发布，未生效
21	《国家网络安全检查操作指南》	中央网络安全和信息化领导小组办公室、网络安全协调局	2016-6	非法律文件

22	《信息安全技术 关键信息基础设施安全检查评估指南（征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效
23	《信息安全技术 关键信息基础设施安全保障评价指标体系（征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效
24	《关键信息基础设施识别指南》	国家互联网信息办公室、工信部、公安部门等部门	N/A	制定中
25	《信息安全技术 关键信息基础设施网络安全保护要求》	全国信息安全标准化技术委员会	N/A	制定中
个人信息和重要数据保护制度				
26	《个人信息和重要数据出境安全评估办法（征求意见稿及修订稿）》	国家互联网信息办公室	N/A	正式版未发布，未生效
27	《信息安全技术 数据出境安全评估指南 （征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效
28	《信息安全技术 个人信息安全规范 （征求意见稿及报批稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效
29	《信息安全技术 个人信息去标识化指南》 （征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效
30	《信息安全技术 公共及商用服务信息系统个人信息保护指南》	工业和信息化部	2013-2-1	现行有效
网络产品和服务管理制度				
31	《网络产品和服务安全审查办法（试行）》	国家互联网信息办公室	2017-6-1	现行有效
32	关于发布《网络关键设备和网络安全专用产品目录（第一批）》的公告	工业和信息化部； 公安部； 国家认证认可监督管理委员会； 国家互联网信息办公室	2017-6-1	现行有效
33	《信息安全技术 网络产品和服务安全通用要求 （征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效
34	《信息安全技术 信息技术产品安全检测机构条件和行为准则（征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效
35	《信息安全技术 信息技术产品安全可控评价指标（第1-5部分）（征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效

网络安全事件管理制度				
36	《国家网络安全事件应急预案》	中央网络安全和信息化领导小组办公室	2017-1-10	现行有效
37	《工业控制系统信息安全事件应急管理工作指南》	工业和信息化部	2017-5-31	现行有效
38	《信息安全技术 网络攻击定义及描述规范（征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效
39	《信息安全技术 网络安全事件应急演练通用指南（征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效
40	《信息安全技术 网络安全威胁信息表达模型（征求意见稿）》	全国信息安全标准化技术委员会	N/A	正式版未发布，未生效
41	《信息安全技术 网络安全漏洞发现与报告管理制度》	全国信息安全标准化技术委员会	N/A	制定中

四、 结论

(一) 《网络安全法》的不足之处

《网络安全法》作为中国网络安全领域的第一部综合性的基础法律，仍然存在一些不足之处，有待在今后的立法中进一步完善。其一，《网络安全法》中提出的一些概念的界限比较模糊，如上文中提到的“网络运营者”及“关键信息基础设施”等，虽然立法者在《网络安全法》中模糊这些概念的界限的做法在目前来看是一种更明智的选择，但是，为了将来的准确执法及实务操作，还是需要在后续配套法规中尽快将相关概念的明确定义及界限确定下来。其二，《网络安全法》在明确了其法律调整范围的同时也限制了其法律调整范围。本法第二条规定了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。然而，随着网络空间的国际化趋势，威胁中国国家安全和网络安全的行为并非只存在在中国境内，而目前的《网络安全法》对中国境外的网络安全威胁则无法适用及规制。其三，《网络安全法》中的指导性的条款占比过多，比如

第一章及第二章主要为指导性条款，欠缺实质性内容，这可能会导致将来法律的实施效果不尽理想。

(二) 对《网络安全法》的展望

作为中国第一部网络安全治理领域的基础性法律，《网络安全法》多层面全方位构筑了网络空间的规范设计体系。其施行不仅将极大地促进信息社会的法治文明建设、网络法制化的发展，并对人们的工作生活产生深远的积极影响，同时其施行对于提高中国网络安全保障能力意义重大，是中国在互联网治理的重要组成部分，为中国社会现代化治理和全球互联网治理作出了重大贡献，也为中国参与全球网络空间治理、提升网络空间国际话语权奠定了基础。

虽然《网络安全法》还有一些不足， 但是《网络安全法》的出台对于确立国家网络安全基本管理制度仍然具有里程碑式的重要意义。《网络安全法》只是一个开端，今后必然会有更多的后续的网络领域的立法，与《网络安全法》共同构建起一个完备的网络法律体系，以守护国家、公共、个人的网络安全，打击网络犯罪，促进网络空间的健康、长足发展。

参考文献

中国信息通信研究院互联网法律研究中心，《网络空间法制化的全球视野与中国时间》，法律出版社，2016年。

张平，《网络法律评论》第18卷，北京大学出版社,2016年。

杨合庆，《中华人民共和国网络安全法释义》，中国民主法制出版社，2017年。

杨合庆，《中华人民共和国网络安全法解读》，中国法制出版社，2017年。

徐汉明，《网络安全立法研究》，法律出版社，2016年。

庹继光，“《网络安全法》的治理思路辨析”，‘新闻与法治’，2017年。

宋燕妮，“《网络安全法》开启我国网络立法新进程”，‘信息安全研究’第三卷，2017年。

齐爱民，“论大数据时代数据安全法律综合保护的完善-以《网络安全法》为视角”，‘东北师大学报（哲学社会科学版）’，2017年。
陈璐，“论《网络安全法》对个人信息刑法保护的新启示-以两高最新司法解释为视角”，‘法治研究’，2017年

[Abstract]

A Comprehensive Guide to Cybersecurity Law

Miao, Fei
Kim&Chang, Chinese Attorney

The development of the Network, which has been deeply integrated into our political, economic and social lives, has brought us convenience on the one hand, but on the other hand, cyber threats are increasingly important and strategically relevant in both developed and developing countries. Cyber security is one of the highest priority items on the global policy and national security agendas, and an increasingly challenging policy area for governments. For the purposes of guaranteeing cyber security, safeguarding cyberspace sovereignty, national security and public interest, protecting the lawful rights and interests of citizens, legal persons and other organizations, and promoting the sound development of economic and social informatization, China has developed the Cybersecurity Law, which is the first comprehensive and fundamental law in the field of cyber security in China. The new Cybersecurity Law introduces a number of measures designed to protect the government and individuals from cybercrime and data leakage. These measures include placing obligations on critical information infrastructure

operators, network operators and providers of network products and services to take active steps to protect computer networks from cyber-attacks and protect personal information and important data from being stolen or used for unauthorized purposes.

This essay aims to provide a comprehensive guide to the Cybersecurity Law by interpreting the background of legislative and main articles of the Cybersecurity Law.

Key words : Cyber Security, Cybersecurity Law, Information Security, Information Protection, Critical Information Infrastructure, Cyber Crime, National security