HANDBOOK
OF CYBER
SECURITY LAW

网络安全法适用指南

主　编◎马民虎

中国民主法制出版社
全国百佳图书出版单位

HANDBOOK
OF CYBER
SECURITY LAW

网络安全法适用指南

主编 /
马民虎
——西安交通大学信息安全法律研究中心主任、中国网络空间安全协会网络空间安全法律与公共政策专业委员会主任委员

副主编 /
崔聪聪
——北京邮电大学互联网治理与法律研究中心副主任、中国网络空间安全协会网络空间安全法律与公共政策专业委员会秘书长

黄道丽
——公安部第三研究所副研究员、公安部第三研究所网络安全法律研究中心主任

中国民主法制出版社
全国百佳图书出版单位

图书在版编目（CIP）数据

网络安全法适用指南/马民虎主编. —北京：中国民主法制出版社，2017.11

ISBN 978-7-5162-1708-5

Ⅰ.①网… Ⅱ.①马… Ⅲ.①计算机网络—科学技术管理法规—法律适用—中国—指南 Ⅳ.①D922.170.5

中国版本图书馆 CIP 数据核字（2017）第 290501 号

图书出品人：刘海涛
出 版 统 筹：乔先彪
责 任 编 辑：逯卫光

书名/网络安全法适用指南
WANGLUOANQUANFASHIYONGZHINAN
作者/马民虎 主编

出版·发行/中国民主法制出版社
地址/北京市丰台区右安门外玉林里 7 号（100069）
电话/（010）63055259（总编室） 63057714（发行部）
传真/（010）63056975 63056983
http：// www.npcpub.com
E-mail：mzfz@npcpub.com
经销/新华书店
开本/16 开 787 毫米×960 毫米
印张/23.75 **字数**/360 千字
版本/2018 年 1 月第 1 版 2018 年 1 月第 1 次印刷
印刷/北京中兴印刷有限公司

书号/ISBN 978-7-5162-1708-5
定价/58.00 元

编写说明

《中华人民共和国网络安全法》（本书简称《网络安全法》）是我国指导、规范和保障网络安全工作的基本法，是贯彻落实“总体国家安全观”的网络空间主权宣言，是构建网络空间命运共同体的法治要求，是实现网络强国战略的法治举措。《网络安全法》的适用，首先要深入领会习近平新时代社会主义法治思想，牢牢把握新时代的矛盾焦点，以国际视野看待我国的网络安全威胁，站在中国立场分析国际网络治理关系，正确处理好安全与发展之间的关系，依法理解运营商遵从法规与维护用户数据安全之间的内在需求，这对准确理解网络安全的精髓，推进国家治理体系和治理能力现代化，实现中华民族伟大复兴的中国梦，保障网络安全活动参与者的合法权益，意义重大。

《网络安全法适用指南》立足于《网络安全法》的立法宗旨，恪守法律适用的基本框架，既有对整体法的立法背景、理念和基本原则的展开论述，又有对具体条文的解释学分析，力求言简意赅，便于管理部门、企业、律师、法官等网络参与者的实际使用。本书从构思到成稿经历了非常艰巨的创作过程，感谢宋燕妮、李欲晓的指导和支持。

本书由西安交通大学信息安全法律研究中心马民虎教授领衔创作，北京邮电大学互联网治理与法律研究中心崔聪聪副主任和公安部第三研究所网络安全法研究中心黄道丽主任共同确定大纲，最后由崔聪聪博士统稿，具体分工如下。

导言：黄道丽；

第一章：马民虎、党家玉、梁思雨、赵婧琳；

第二章第一节：陈晓桦、胡文华；

第二章第二节、第五节：赵光；

第二章第三节：张健、胡文华；

第二章第四节：陈晓桦、何治乐；

第二章第六节：张健；

第三章第一节、第六节、第七节：黄道丽；

第三章第二节：何治乐；

第三章第三节：黄道丽、胡文华；

第三章第四节：赵丽莉、胡文华；

第三章第五节：方婷；

第三章第八节：原浩；

第四章第一节：崔聪聪；

第四章第二节：赵光、弟莉莉；

第四章第三节：马宁；

第四章第四节：马宁、方婷；

第四章第五节：马宁、张若琳；

第四章第六节：原浩；

第五章：方婷；

第六章第一节、第二节、第四节、第五节、第六节：崔聪聪；

第六章第三节：马可、赵光；

第七章第一节、第二节、第四节：李海英；

第七章第三节：程程；

第八章：方婷；

第九章：王玥、赵光；

第十章：果园；

第十一章第一节：缐金伟；

第十一章第二节：原浩；

第十一章第三节：黄道丽、原浩、冯潇洒；

附录一：何治乐；附录二：冯潇洒、梁思雨；附录三：胡文华；附录四：冯潇洒；附录五：马民虎、李菁菁、左晓栋等；附录六：黄道丽、何治乐、原浩。

本书编写时间仓促，书中难免出现疏漏乃至错误之处，恳请读者批评指正！

编者

2017 年 10 月

目　录

Contents

导　言

一、立法背景

自20世纪80年代以来，网络技术的快速发展和广泛应用，引发了一场新的全球性产业革命，网络空间逐渐被视为继陆、海、空、天之后的“第五空间”。信息化成为当今世界发展的主要趋势，也成为推动经济发展和社会变革的重要力量。然而，信息化带来的网络安全威胁范围和内容也不断扩大和演化，全球网络安全形势与挑战日益严峻，正如尼古拉斯·尼葛洛庞帝在《数字化生存》中所言，“每一种技术或科学的馈赠都有其黑暗面”。世界各国纷纷将网络安全提升到国家战略高度，目前有七十多个国家制定了网络安全方面的国家战略，各国网络安全相关政策立法也呈爆发趋势。全方位、更立体、更具弹性与前瞻性的网络安全政策立法体系正在构建。

在2015年颁布《美国网络安全法》（Cyber Security Act of 2015）之后，美国接连通过多部网络安全政策法规，以加强美国网络安全和抵御网络攻击的能力，包括2016年通过的《信息自由法案促进法》（FOIA Improvement Act of 2016）、国防部《安全漏洞披露政策》（Vulnerability Disclosure Policy）、《波特曼-墨菲反宣传法案》（Portman-Murphy Counter-Propaganda Bill），2017年的《国家网络事件响应计划》（The National Cyber Incident Response Plan）、《2017NIST网络安全框架、评估和审查法案》（NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017）和司法部《在线系统漏洞披露计划框架》（A Framework for a Vulnerability Disclosure Program for Online Systems）。此外，2017年5月11日，美国总统特朗普签署了第一份网络安全行政令——《增强联邦政府网络与关键性基础设施网络安全》的总统行政令（Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure），其中要求美国采取一系列措施来增强联邦政府、关键基础设施和国家这三个领域的网络安全。

欧盟一直致力于实现统一的、高水平的网络与信息系统安全，在2016

年7月通过第一部网络安全法案——《网络与信息系统安全指令》，并要求欧盟成员国必须在21个月内将其转化为国内法。英国于2016年年底颁布史上最严协助执法法——《调查权利法案》（Investigatory Powers Bill），旨在进一步厘清执法机构在通信及通信数据拦截、获取、留存及设备干扰等方面的权力，由此帮助执法机构调查犯罪和防控恐怖主义。

俄罗斯于2015年发布新版战略《俄罗斯联邦信息安全学说》，这也是自2000年以来俄罗斯首次对国家信息领域战略的更新，提出了俄罗斯面临的10个方面的信息安全威胁。此外，2017年7月，俄罗斯发布《俄罗斯联邦信息基础设施安全法》，该法明确了俄罗斯联邦关键信息基础设施安全保障领域的联邦执行机关，并明确构建关键信息基础设施分级标准、标准指标以及分级制度来确保俄罗斯关键信息基础设施的安全。

我国同样面临着更为复杂的安全威胁。国内网络安全威胁和风险日益突出，并日益向政治、经济、文化、生态、国防等领域传导渗透；境外敌对势力把我国作为网络意识形态渗透与攻击的重点；网络空间主导权争夺激烈，而数据跨境流动的监管缺失直接威胁我国网络主权和国家司法权力架构；多网域“跨际”和“供应链渗透”威胁着工控、能源、交通、金融、电力等关键信息基础设施的安全；境内大规模个人信息泄露事件不断发生，网络诈骗、非法入侵、系统攻击等更加频繁，严重威胁社会公共安全和个人的合法权益。

“没有网络安全就没有国家安全，没有信息化就没有现代化”，国家加快开启了网络强国建设的顶层设计和一系列战略部署。2014年2月27日，中央网络安全和信息化领导小组正式成立，这标志着我国正式将网络安全提升至国家安全的高度，构筑全方位的网络与信息安全治理体系成为我国网络安全保障工作的重中之重。2016年7月，中共中央办公厅、国务院办公厅发布《国家信息化发展战略纲要》（以下简称《纲要》）。作为规范和指导我国未来10年国家信息化发展的纲领性文件，《纲要》进一步调整和发展了中期国家信息化发展战略，其中要求以信息化驱动现代化，加快建设网络强国。2016年12月27日，我国《国家网络空间安全战略》正式发布，这是我国第一次向全世界系统、明确地宣示和阐述我国对于网络空间安全和发展的立场与主张，在我国网络空间安全领域具有里程碑意义。2017年3月1日，外交部和国家互联网信息办公室共同发布《网络空间国际合作战略》，全面宣示了我国在网络空间国际治理问题上的基本原则和行动要点。这三个战略开启

了我国网络空间治理的全新范式，为我国网络安全相关政策和法律的出台指明了方向。

纵观我国网络空间领域的立法进程，2012 年是一个重要分水岭。2012 年之前颁布施行的信息安全立法，涉及了法律、行政法规、部门规章、地方法规及规范性文件等多个层次：从涉及的领域来看，具体包括网络与信息系统安全、信息安全系统与产品、信息内容安全、保密及密码管理、计算机病毒防治等多个领域；从权利（力）角度来看，主要包括政府维护信息安全的职责、企业权益保障和个人信息权利保护等。这些法律相比于国际立法，内容相对滞后，且各法律文件之间相互独立，呈碎片化，由此构建的信息安全立法框架显然无法有效地应对日渐严峻的网络安全威胁。能源、交通、金融、电力等国家关键信息基础设施建设、管理法制不健全，信息安全技术研究和产品开发政策法律保障乏力，在发生重大、突发事件和紧急状态情况下，应急响应缺乏法律保障，应急预案、违法犯罪信息和安全测试等可以用于社会安全防范的信息难以共享，严重影响了网络空间的快速反应能力、安全保障能力和统一调配能力。

面对严峻的网络安全形势，社会各界普遍认为，仅对原有法律的解释、修订或增补，难以把握好安全与发展之间的关系，不利于国家总体安全战略目标的实现，我国亟需制定综合性“网络领域基本法”，应当明确规定网络与信息安全的基线，为部门、地方的立法和政策的制定、调整和完善提供法律依据。2013 年下半年，网络安全立法提上日程。2014 年 4 月，全国人大常委会年度立法计划正式将《网络安全法》列为立法预备项目，由此开启了我国国家网络安全立法的新进程。2015 年 7 月 6 日，作为网络安全基本法的《网络安全法（草案）》第一次向社会公开征求意见；2016 年 11 月 7 日，第十二届全国人民代表大会常务委员会第二十四次会议表决通过了《网络安全法》，并于 2017 年 6 月 1 日正式施行。《网络安全法》的实施，标志着我国网络空间法制化进程的实质性展开，为我国有效应对网络安全威胁和风险、全方位保障网络安全提供了基本法律支撑。

二、立法理念

“法律制定及运用之最高原理，谓之法律之理念；法律之理念，为法律的目的及手段之指导原则”。法律理念是对法律的本质及其发展规律的一种宏观的、整体的理性认知和把握。法律理念比法律观念、法律概念和法律意识等

的层次更高，可为法律制定和实施提供科学指导。现代法的法律理念包括了正义、民主、平等、法治、权利、安全、效益和可持续发展等。

随着网络信息技术的不断发展，我国国家关键基础设施越来越依赖网络，关键信息基础设施关涉国家安全和社会稳定，是网络安全的重中之重。习近平总书记审时度势，提出了“坚持总体国家安全观，走中国特色国家安全道路”的新观点，强调国家的安全发展要同时兼顾外部安全与内部安全、国土安全与国民安全、传统安全与非传统安全、发展问题与安全问题、自身安全与共同安全。“总体国家安全观”强调了更深、更高、更全面的综合安全，创造性地提出了富有中国特色的国家安全价值观念、工作思路与机制路径。

“总体国家安全观”为我国《网络安全法》的制定和实施工作提供了科学的理念指导，符合“总体国家安全观”要求的网络安全是国内外复杂开放环境下的网络安全，不是碎片化、局域化、区域化的网络安全。《网络安全法》继承了既重视发展问题，又重视安全问题；既重视自身安全，又重视共同安全的核心理念，统筹把握国家安全与网络安全、网络安全与信息化发展、国内治理与国际合作等关系，体现了整体、动态、开放、相对、共同的网络安全观，为新时期网络安全工作指明了方向。

三、立法定位

科学的立法定位是搭建立法框架与设计立法制度的前提条件，立法定位对于法的结构确定起着引导作用，为法的具体制度设计提供法理上的判断依据。2015 年 7 月 6 日，全国人大常委会发布的《关于〈中华人民共和国网络安全法（草案）〉的说明》中确立了“坚持从国情出发、坚持问题导向和坚持安全与发展并重”的立法三原则。在坚持问题导向原则的指导下，该说明特别强调：“本法是网络安全管理方面的基础性法律，主要针对实践中存在的突出问题，将近年来一些成熟的好做法作为制度确定下来，为网络安全工作提供切实法律保障。对一些确有必要，但尚缺乏实践经验的制度安排做出原则性规定，同时注重与已有的相关法律法规相衔接，并为需要制定的配套法规预留接口。”由此可以看出，《网络安全法》是定位于网络安全管理的基础性“保障法”。

第一，该法是网络安全领域的基础性法律。基础性法律的功能不是重在解决具体问题，而是为问题的解决提供具体指导思路。问题的解决要依靠相

配套的法律法规，这样的定位不可避免地会出现法律表述上的原则性，相关主体只能判断出网络安全管理对相关问题的解决思路，具体的解决办法有待其他法律法规进行细化。

第二，该法是网络安全保障法。2010 年之后各国陆续出台的第二代网络安全政策立法普遍体现出安全保障法的特征，即以发现、消除网络安全威胁和风险，提升恢复能力为轴心。“发现”强调网络安全漏洞的掌控、网络安全威胁和风险信息的实时全面共享、侦查、监测预警和供应链安全等；“消除”强调及时动态地研判处置网络攻击，实施精准打击的同时允许有条件的攻击反制；“恢复”侧重网络安全态势感知和网络攻击之后的应对恢复，保护有关各方的合法权益，提升各方对国家安全和社会稳定的信心。

第三，该法是网络安全管理的法律。《网络安全法》与《国家安全法》、《反恐怖主义法》、《刑法》、《保守国家秘密法》、《治安管理处罚法》、《关于加强网络信息保护的决定》、《关于维护互联网安全的决定》、《计算机信息系统安全保护条例》、《互联网信息服务管理办法》等法律法规共同组成我国网络安全管理的法律体系。因此，须做好《网络安全法》与不同法律之间的衔接，在网络安全管理之外的领域也应尽量减少交叉与重复。

四、立法机制

面对网络空间安全的综合复杂性，特别是国家关键信息基础设施面临日益严重的传统安全与非传统安全的“极端”威胁，网络空间安全风险“不可逆”的特征进一步凸显。在开放、交互和跨界的网络环境中，实时性能力和态势感知能力成为新的网络安全核心内容。在这样的背景下，传统上将风险预防寄托于惩治的立法理念将面临挑战。

为实现基础性法律的“保障”功能，《网络安全法》以“预防和控制”性的法律规范替代传统单纯“惩治”性的刑事法律规范，从政府、企业和个人等多方主体参与综合治理的层面，明确了各方主体在预警与监测、网络安全事件的应急与响应、控制与恢复等环节中的过程控制要求，同时不断加大对相关违法行为的处罚力度，维护网络空间安全和秩序，已开始摆脱传统上将风险预防寄托于事后惩治的立法理念，预防、控制、合理分配安全风险，其配套制度的制定与出台正在不断夯实这一“预防、控制与惩治”立法架构。

五、立法特点

（一）战略入法

目前，网络安全已经上升到国家核心战略层面，成为国家安全的基础性保障。在认识到当前网络安全动态、开放、相对、共同的特征后，《网络安全法》践行总体国家安全观，从宏观层面明确提出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。《网络安全法》第二十四条进一步明确提出国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。在鉴别用户身份的基础上，把个人、机构和设备有机地结合在一起，以保证用户交易时的安全，整合互联网资源，建立由政府主导、市场经济主体推动的可信身份制度，促进网络空间身份管理的发展，将可信身份在基本法层面上升到国家战略高度，为出台相关政策措施提供了法律依据。

（二）立法首次采用“关键信息基础设施”概念

关键信息基础设施保护制度是《网络安全法》核心制度。近年来，世界主要国家和地区都陆续出台了国家层面的关键信息基础设施保护战略、立法和具体的保护方案，以美国为主的西方国家都将关键信息基础设施的保护视为网络安全的最核心部分。

《网络安全法》在“网络运行安全”一般规定的基础上设专节规定了关键信息基础设施保护制度，首次从网络安全保障基本法的高度提出关键信息基础设施的概念，并提出了关键信息基础设施保护的具体要求。

《网络安全法》中明确界定了关键信息基础设施概念的本质，即“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”，并规定关键信息基础设施的具体范围由国务院另行制定。这表明，作为网络安全领域的基本法，应当尽可能确保《网络安全法》的稳定性而不宜进行过于细化的条款设定这一立法需求。而关键信息基础设施的范围将基于国家安全和社会运行的风险评估进行不断调整，即其认定范围遵循动态调整机制。

关键信息基础设施安全保护办法是《网络安全法》中预留接口的下位法，也是法律中唯一明确规定“由国务院制定”的行政法规。我国关键信息基础

设施法律制度在法律调整的社会关系及调整对象上更具复杂性。政治、法律传统等国情的差异导致我国关键信息基础设施保护制度的构建不能简单照搬外国的经验，应坚持国内经验总结和国外经验借鉴相结合，建立符合我国国情且具有较强操作性的关键信息基础设施保护制度，同时也科学合理地推动网络安全等级保护制度的演进与变革，实现制度间的互补和融合，降低关键信息基础设施运营者的守法成本和行政执法成本。

（三）多层次责任主体的双面规范架构

习近平总书记在主持“4·19”座谈时明确指出：“维护网络安全是全社会共同责任，需要政府、企业、社会组织、广大网民共同参与，共筑网络安全防线。”为了切实形成全社会共同维护网络安全的强大合力，《网络安全法》构建了政府、组织和个人的多层次责任主体架构，针对不同责任主体给予相对应的发展和保障措施。

从政府层面，《网络安全法》覆盖国家网信部门、国务院电信主管部门、公安部门、关键信息基础设施安全保护工作部门、国务院标准化行政主管部门、县级以上地方人民政府有关部门等主体。《网络安全法》一方面明确网络安全监管体制，理顺各部门之间的权力范围，赋予其维护网络安全、惩治网络违法犯罪的权力；另一方面，通过强化法律责任和社会监督，限定权力边界，推进国家治理体系和治理能力现代化。

从组织层面，《网络安全法》覆盖网络运营者、网络产品和服务提供者、关键信息基础设施运营者、个人和组织、电子信息发送服务提供者、应用软件下载服务提供者、网络安全服务机构、网络相关行业组织、研究机构、企业、高校、大众传播媒介等主体，一方面明确特定组织的网络安全保护义务和合规要求，强化社会责任，实施信用惩戒，加大对组织违法行为的处罚力度；另一方面，鼓励支持企业创新，加强政企合作，支持企业、研究机构、高等院校、行业组织等参与标准制定，支持开展网络安全相关教育与培训，支持多种方式培养网络安全人才，促进经济社会信息化健康发展。

从个人层面，《网络安全法》一方面保护个人依法使用网络的权利，赋予其社会监督权利，突出未成年人保护，全生命周期强化个人信息保护；另一方面，倡导社会主义核心价值观，行刑衔接划定个人实施网络安全活动的界限，规范个人网络信息内容，创设从业禁止规定，加大对个人违法行为的处罚力度。

《网络安全法》对多层次责任主体的双面规范有助于各级政府和各行

业、各领域加强对网络安全保护、网络安全教育、网络安全宣传、网络安全产业的统筹规划；有助于促使全社会提升对网络安全保护工作重要程度的认知，系统和全面认识网络安全保护工作体系、工作内容和工作措施，提升开展网络安全保护工作的能力；有助于个人提高网络安全意识，增强自我保护能力，降低个人实施危害网络安全行为的可能性，提升全社会网络安全保护水平。

第一章

总　则

核心内容

1. 《网络安全法》的立法目的
2. 《网络安全法》的适用范围
3. 网络安全管理工作的方针和原则
4. 网络安全管理工作体制
5. 网络行为规范
6. 国际网络治理体系

本章综述

总则是整部《网络安全法》的灵魂所在，确立了我国网络安全保障的根本目的和基本原则，明确了我国网络空间治理的政策定位和发展策略。在总则中，《网络安全法》将保障网络安全，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作为网络安全立法的核心价值和根本目的。同时，以法律的形式确立了国家网络安全保障工作的基本原则和政策方针：坚持安全与发展并重的安全保障原则，遵循积极利用、科学发展、依法管理、确保安全的政策方针。在国家网络安全保障的具体策略方面，总则规定国家制定并不断完善网络安全战略，采取措施监测、防御和处置网络安全风险和威胁，依法惩治网络违法犯罪活动，通过提高全社会网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。同时，积极开展网络安全治理的国际交流与合作，建立多边、民主、透明的网络治理体系。在鼓励合法使用的前提下，《网络安全法》总则建立了我国网络安全保障的基本规则框架，明确了包括政府、网络运营者、行业组织以及公民、法人和其他组织等主体在内的权利义务关系。此外，《网络安全法》总则特别强调对未成年人的保护工作，