COMPLIANCE
OF CYBER
SECURITY LAW

网络安全法律遵从

马民虎◎主编

360法律研究院◎组织编写

中国工信出版集团

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

COMPLIANCE
OF CYBER
SECURITY LAW

网络安全法律遵从

马民虎◎主编

360法律研究院◎组织编写

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书针对企业网络安全法律遵从的实际需求，以《中华人民共和国网络安全法》（以下简称《网络安全法》）为分析蓝本，从相关法条释义和解读、网络安全相关制度概述、典型案例解析等方面，梳理和分析了一般网络运营者、关键信息基础设施运营者，以及网络产品和服务提供者的网络安全法律遵从框架与实施建议，以期为相关企业遵从《网络安全法》及其制度要求提供可操作性指引。本书分为四个部分，分别是《网络安全法》导论、一般网络运营者的网络安全法律遵从、关键信息基础设施运营者的网络安全法律遵从及网络产品和服务提供者的网络安全法律遵从。

图书在版编目（CIP）数据

网络安全法律遵从/马民虎主编. —北京：电子工业出版社，2018.2
ISBN 978-7-121-33249-4

Ⅰ. ①网… Ⅱ. ①马… Ⅲ. ①计算机网络－科学技术管理法规－中国 Ⅳ. ①D922.17

中国版本图书馆 CIP 数据核字（2017）第 306228 号

策划编辑：戴晨辰
责任编辑：戴晨辰　　文字编辑：韩玉宏
印　　刷：三河市双峰印刷装订有限公司
装　　订：三河市双峰印刷装订有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：720×1 000　1/16　印张：28.75 字数：499 千字
版　　次：2018 年 2 月第 1 版
印　　次：2018 年 2 月第 1 次印刷
定　　价：79.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：dcc@phei.com.cn。

编委会

Editorial Committee

（按姓氏笔画排序）

前言

Preface

网络安全事关国家利益，而网络空间中的国家利益冲突极其尖锐，其中军事冲突、进出口管控，以及国家安全审查、数据主权等方面的国际斗争日趋激烈。在互联网迅速发展的时代，网络安全已成为影响国家安全和社会稳定的关键问题，成为国家安全体系的重要组成部分。网络安全和信息化对一个国家的很多领域来说都是牵一发而动全身的，没有网络安全就没有国家安全。鉴于网络安全在国家安全中的重要性，以及网络安全面临的复杂形势，制定网络安全法，提高网络治理的法治化水平已是必然。

2016年11月7日，第十二届全国人民代表大会常务委员会（以下简称“全国人大常委会”）第二十四次会议通过《中华人民共和国网络安全法》（以下简称《网络安全法》），并于2017年6月1日起正式实施，共7章，79条。《网络安全法》是我国信息安全领域的重大立法，它体现了国家对建立健全网络空间秩序的基本意志。该法确立了“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、法人和其他组织合法权益，促进经济社会信息化健康发展”的立法目标，调整范围包括中华人民共和国境内建设、运营、维护和使用的网络，以及网络安全的监督管理，具体内容涉及网络安全支持与促进、网络运行安全、网络信息安全、监测预警与应急处置、法律责任等方面。《网络安全法》的制定和实施响应了习近平总书记提出的“全天候全方位感知网络安全态势”的基本要求，是依法治网的一个重大立法举措，弥补了网络安全法律保障机制上位法

律制度的缺失，对配套法律法规的制定和具体制度的实施具有重要的指导作用。

本书以《网络安全法》为分析蓝本，以企业网络安全法律遵从为视角，围绕《网络安全法》相关法条释义和解读、网络安全相关制度概述、典型案例解析等方面，梳理和分析了一般网络运营者、关键信息基础设施运营者，以及网络产品和服务提供者这三类遵从主体的网络安全法律遵从框架和实施建议，以期为相关企业遵从《网络安全法》及其制度要求提供可操作性指引。本书框架由方婷、郑蕾、赵军、张素伦共同讨论，章节框架最后由马民虎、许坚确定，方婷、郑蕾统筹实施，书稿分为以下四个部分。

第一部分（第 1 章～第 4 章）为《网络安全法》导论。该部分重点梳理和分析了国内外网络安全态势、国内外网络安全事件与立法，以及《网络安全法》的基本原理。马民虎、方婷、梁思雨、张若琳、马可、张敏、党家玉负责本部分的撰写工作。

第二部分（第 5 章～第 12 章）重点分析了一般网络运营者的网络安全法律遵从。该部分分别从网络安全等级保护制度，网络实名制，网络安全监测预警和应急响应，安全认证、检测及风险评估，网络安全信息披露，协助执法，个人信息保护，以及网络信息内容过滤等方面分析已有网络安全法律制度对一般网络运营者提出的法律遵从要求。黄道丽、王玥、赵丽莉、李海英、方婷、赵光、何治乐、唐治国、马可、冯潇洒、党家玉、梁思雨负责本部分的撰写工作。

第三部分（第 13 章～第 17 章）重点分析了关键信息基础设施运营者的网络安全法律遵从。该部分首先对关键信息基础设施的界定及其范围进行解读，并进一步针对关键信息基础设施运营者的安全保护义务、网络安全审查要求、数据本地化与跨境传输要求、网络安全信息共享要求等提出我国关键信息基础设施运营者的网络安全法律遵从框架及建议。赵婧琳、张敏、马宁、郑蕾、梁思雨、方婷和马悦负责本部分的撰写工作。

第四部分（第 18 章～第 22 章）重点分析了网络产品和服务提供者的网络安全法律遵从。该部分在对《网络安全法》关于网络产品和服务提供者规定的基础上，围绕网络产品和服务安全、网络安全漏洞通知和报告、用户信息保护、保密义务、网络关键设备和网络安全专用产品强制认证等方面重点分析了网络产品和服务提供者的网络安全法律遵从框架及建议。黄道丽、方婷、江智茹、党家玉、张若琳、梁志伟负责本部分的撰写工作。

目录

Contents

第一部分 《网络安全法》导论

第三部分　关键信息基础设施运营者的网络安全法律遵从

第四部分 网络产品和服务提供者的网络安全法律遵从

Part 1

第一部分

《网络安全法》导论

第 1 章

国内外网络安全态势

人类社会发展至今，先后经历了农业革命和工业革命，当前正在历经信息革命。信息革命作为经济全球化的重要推动力量，引领了社会生产新变革，创造了人类生活新空间，拓展了国家治理新领域，极大地提高了人类认识世界、改造世界的能力。随着全球信息化的发展和深入推进，网络与经济社会各领域深层次融合，网络在极大地促进经济社会繁荣进步的同时，其带来的安全威胁和风险也日益突出，特别是针对关键信息基础设施的重大网络安全事件，例如，针对乌克兰电网发起的攻击造成基础电力运行的崩溃；针对伊朗核设施的攻击使其被迫暂停核运行；针对美国 Dyn 域名服务提供商进行的分布式拒绝服务（Distributed Denial of Service，DDoS）攻击使大量网站陷入瘫痪，造成的灾难性后果已严重危害国家经济安全和公共利益。与此同时，网络恐怖主义、网络诈骗、网络谣言等的恶意蔓延也直接威胁人们的生命财产安全，影响社会和谐稳定，长此以往将导致人们对网络安全的不信任，抑制信息化的发展。因此，网络安全已经成为事关人类共同利益，事关世界和平与发展，事关国家安全的重要一环。

近年来，新一代信息技术蓬勃发展，大数据、云计算、物联网等在带来便利的同时，也引发了新的网络安全问题。云计算需要汇集海量的数据从而进行整合处理，使得数据的跨境流动成为常态，数据主体对于数据资源的控制力持续削弱。“棱镜门”事件的爆发使得各国开始意识到此种削弱使得数据本身的安

全性和由数据所承载的国家安全、社会稳定和个人信息都面临潜在威胁，数据的主权界定也就成为亟待解决的问题。与此同时，各国政府和私有部门纷纷在物联网和人工智能等新兴信息技术领域投入更多资源，使其逐渐成为恶意网络分子利用的工具，网络攻击手段更加复杂，溯源难度进一步增加，而物联网和人工智能技术本身引起的隐私保护和道德伦理等问题也摆在眼前。因此，无论是出于保护传统网络安全，还是维护新兴技术发展的目的，各国都充分认识到网络安全对于国家、社会和公民的价值，普遍将其提升到国家战略层面，并且针对关键信息基础设施、网络恐怖主义、网络谣言及数据保护等内容完善立法，同时，加强国际合作，提升网络空间的国际话语权，构建网络空间国际治理规则。

态势一：各国普遍将网络安全提升到国家战略层面

网络空间已经成为与海、陆、空和外层空间同等重要的人类活动新领域。在国际社会，对于网络这一第五空间的关注从未停止，国家政治、经济、文化、国防及公民在网络空间的合法权益皆面临严峻挑战。近年来，各国在推动网络核心技术、新兴技术发展的基础上，将安全理念从局部安全拓展为全面安全，将中长期发展战略、网络安全人才培养、国际合作等内容也囊括在内。我国于 2014 年提出总体国家安全观，将国家安全置于国家治理的大背景下来思考和筹划，将安全治理作为基本路径来维护和保障。坚持总体国家安全观，体现在治理实践上，就是推进国家安全总体治理；既重视传统安全，又重视非传统安全，构建集政治安全、国土安全、军事安全、经济安全、文化安全、社会安全、科技安全、信息安全、生态安全、资源安全、核安全等于一体的国家安全体系；走出一条中国特色国家安全道路，在安全各领域、各要素、各层面统筹治理，创建当代中国国家安全治理系统格局。

国际社会中，2011 年，美国出台《网络空间国际战略》（International Strategy for Cyberspace）宣称要建立一个“开放、互通、安全和可靠”的网络空间，并为

实现这一构想勾勒出了政策路线图，内容涵盖经济、国防、执法和外交等领域。

近几年美国又先后公布《网络空间政策审查》（Cyberspace Policy Review）、《国际网络战略网络世界的繁荣、安全和开放》（International Strategy for Cyberspace: Prosperity，Security，and Openness in a Networked World）、《改善关键基础设施网络安全的行政令》（Improving Critical Infrastructure Cybersecurity）、《2014 年网络安全增强法案》（Cybersecurity Enhancement Act of 2014）、《2014 年国家网络安全保护法》（National Cybersecurity Protection Act of 2014）、《改进关键基础设施网络安全草案》（Draft Strategy for Improving Critical Infrastructure Cybersecurity）、《国家安全战略》（National Security Strategy）、《国防部网络战略》（The Department of Defence Cyber Strategy）、《2015 年网络安全法案》（Cybersecurity Act of 2015）、《增强联邦政府网络与关键基础设施网络安全的行政令》（Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure）等一系列法律规范和政策，着眼于在提升网络安全应急和防御能力的同时建立本国的网络部队，同步培育自卫能力和对外威慑力。

与此同时，欧盟也颁布《欧盟网络安全战略：公开、可靠和安全的网络空间》（Cybersecurity Strategy of the European Union: An Open，Safe and Secure Cyberspace）、《欧盟网络防御政策框架》（EU Cyber Defence Policy Framework）、《欧洲安全议程》（The European Agenda on Security）、《欧洲议会和欧盟理事会关于自然人个人数据处理和数据自由流动保护，并废除 95/46/EC 号指令的第 2016/680 号条例（通用数据保护条例）》[①]、《欧盟网络与信息系统安全指令》（The Directive on Security of Network and Information Systems）、《欧洲议会和欧盟理事会关于欧盟高级别网络和信息系统安全措施的第 2016/1148 号指令》[②]等，强调成员间、成员内部政府、企业和社会服务等机构之间的信息共享与交流合作，致力于共同维护网络安全。

逐渐脱欧的英国为保障本国在数据时代的安全和繁荣，先后公布《动荡时代

① Directive（EU）2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data，and repealing Directive 95/46/EC（General Data Protection Regulation）.

② Directive（EU）2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.