

珞珈网络治理文库

网络安全的 法律治理

袁康 主编



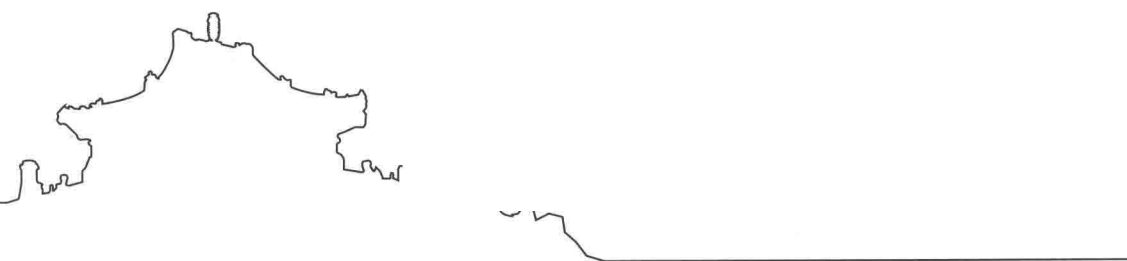
WUHAN UNIVERSITY PRESS
武汉大学出版社



珞珈网络治理文库

网络安全的 法律治理

袁康 主编



WUHAN UNIVERSITY PRESS

武汉大学出版社

图书在版编目(CIP)数据

网络安全的法律治理/袁康主编.—武汉:武汉大学出版社,2020.11
珞珈网络治理文库

ISBN 978-7-307-21823-9

I.网… II.袁… III.计算机网络—科学技术管理法规—研究—中国
IV.D922.174

中国版本图书馆 CIP 数据核字(2020)第 193691 号

责任编辑:胡 荣 责任校对:汪欣怡 整体设计:韩闻锦

出版发行:武汉大学出版社 (430072 武昌 珞珈山)

(电子邮箱:cbs22@whu.edu.cn 网址:www.wdp.com.cn)

印刷:武汉鑫佳捷印务有限公司

开本:720×1000 1/16 印张:34.75 字数:586千字 插页:3

版次:2020年11月第1版 2020年11月第1次印刷

ISBN 978-7-307-21823-9 定价:149.00元

版权所有,不得翻印;凡购我社的图书,如有质量问题,请与当地图书销售部门联系调换。



编委会

主任：冯 果 王中桥

委员：（以姓氏笔画为序）

王中桥 冯 果 皮 勇

孙 晋 张 鹏 杨恒敏

赵 波 袁 康 黄志雄

网络安全法律治理体系的四个层次 (代序)

信息技术的发展和应用的不断深入，为经济社会进步和民族复兴带来了千载难逢的历史机遇。然而，日益突出的网络安全威胁和风险，正以隐蔽化、多样化、复杂化的形态挑战着网络空间秩序和公私利益。习近平总书记指出，没有网络安全就没有国家安全，就没有经济社会的稳定运行，广大人民群众利益也难以得到保障。因此网络安全治理事关国家安全和经济社会发展的大局，事关国家利益和人民群众的根本利益，是网络空间治理的首要任务。在网络安全形势日益严峻的背景下，以《网络安全法》为基础进一步构建和完善网络安全法律治理体系，确保互联网在法治轨道上健康运行，是提高治网管网能力、依法维护网络安全的重要保障。

实施法律治理是维护网络安全的必要手段。网络安全风险的形成，既有技术不完备或系统漏洞等客观原因，也有相关主体不作为或恶意行为等主观原因，同时还受到政治、经济和社会等方面的不确定因素影响。因此网络安全问题不只是技术问题，还是社会关系冲突在网络空间的反映。系统优化、漏洞修复、防火墙、数据加密、身份认证等技术治理手段可以成为维护网络安全的直接策略，但却无法有效回应和调节其背后的社会关系冲突和利益博弈，也因缺乏普遍性和强制性的制度依据而难以全面落实。因此，维护网络安全不仅需要技术理性也需要制度理性，法律治理与技术治理是网络安全治理一体之两翼。按照法律治理路径，通过明确网络空间主体权利义务与责任、规范和约束网络运行和服务过程中的行为、构建有效的监管框架和规则体系，以法律手段和法治思维有效调节网络空间活动中的社会关系和主体行为，并将技术规范上升为具有普遍约束力的法律规则，从而形成全面、充分且有效的网络安全法律治理

体系。

网络安全法律治理体系需要基于技术规律和法治规律进行层次化构建。逻辑清晰、覆盖全面、科学合理、层次分明的制度体系，能够为相关主体及其行为提供明确法律依据以实现指引、预测和评价等效果，是实施有效法律治理的前提和保障。尽管从技术角度对网络层次划分有不同类型，但在治理视角下可以根据技术环节和功能特征的差异，将网络空间归纳为提供物理支撑和系统支持的基础层、提供连接服务和信息传输的网络层和提供内容处理和服务的应用层，相应的网络安全应当包括基础层安全、网络层安全和应用层安全等范畴。从法治规律来看，对网络安全的治理需要明确调整对象、法律主体、行为模式和法律后果，围绕主体、权利、义务、责任进行制度设计。因此，结合技术实现和社会关系调节的层次、重点和路径，可以从基础设施、主体、内容和行为四个层次构建网络安全法律治理体系。位于基础层和网络层的基础设施、位于应用层的数据和信息服务等内容以及贯穿于各层的网络空间主体及其行为，能够作为并列的调整对象在网络空间法律治理体系中实现有机统一。

首先，应在基础设施层次加强网络安全的法律治理。基础设施是为网络运行提供物理支撑和信息通信交互的软硬件集合，一旦基础设施遭到攻击或者破坏，将会导致网络瘫痪甚至严重影响国家安全、经济安全以及社会稳定。基础设施安全包括网络基础设施安全和关键信息基础设施安全。前者主要指光缆光纤、移动通信基站、数据中心、IP 地址与域名等互联网核心架构的安全稳定，是公共网络能够正常运行的基本保障。后者则是金融、能源、通信、电力等关键领域的和其他一旦遭到破坏、丧失功能或数据泄露可能产生严重危害的网站、平台和系统等。基础设施安全是网络安全重中之重，因此需要将基础设施作为重点对象，以专门的法律制度对其进行特殊保护。具体而言，需要通过立法推动我国网络基础设施自主发展，以市场准入制度和安全审查制度确保基础设施的自身安全自主，同时建立关键基础设施安全评估与预警制度，加强和完善基础设施安全分级保护制度，以实现我国网络基础设施和关键信息基础设施的安全可信、稳定可靠和自主可控。

其次，应在主体层次加强网络安全的法律治理。尽管网络空间是虚拟的，但运用网络空间的主体是现实的。网络空间主体涵盖了政府、企业、行业协会、用户等诸多利益相关方，而这些主体参与网络空间活动的立场、习惯和行为习惯都会在不同程度对网络安全造成影响。抓住网络空间主体这个“牛鼻

子”，明确各方权利义务和主体责任，是网络安全法律治理的关键。法律应当明确网络安全治理中的政府角色和监管机制，理顺网络安全治理的职权归属和范围，强化政府相关部门在促进、支持和维护网络安全方面的行政权力与责任，提高网络安全监管执法的能力与效率。同时需要明确网络运营者、网络产品和服务提供者等企业以及网络用户的权利与义务，赋予行业协会和技术社群的自律监管和安全监督的权利和责任，充分调动各类主体维护网络安全的积极性和责任感，鼓励形成捍卫网络安全的社会力量，为各类主体共筑网络安全防线赋能。

再次，应在内容层次加强网络安全的法律治理。内容是网络在应用层运行的最终表现，包括提供的产品与服务、交互的数据和信息等。内容的安全直接关系到网络用户的人身财产利益，直接关系到网络空间的秩序稳定，直接关系到网络活动的经济社会效益，必须将其纳入网络安全法律治理体系之中。当前内容安全领域最为严峻的挑战是数据安全、个人信息保护、网络交易安全以及网络意识形态安全。对此，需要进一步明确数据权属和数据安全管理制度，强化和落实数据安全保护责任和数据采集、存储、使用和转移规则，建立公共数据开放和隐私数据保护的差异化制度，完善数据合规体系。同时，要完善电子商务、互联网金融等交易领域的身份验证、信息加密、信用评价等安全管理的规则与标准。对于因技术和模式创新所形成的新型应用，需要建立风险评估与安全审查制度，并且结合其风险特征及时建立有针对性的监管规则。此外，要按照总体国家安全观的要求加强网络空间内容治理，增强主流意识形态在网络信息传播和网络文化中的引领作用和主导地位，以法律规范清晰划定网络信息的政治底线和道德底线，以健全的综合治理机制为网络意识形态安全营造风清气正的网络生态。

最后，应在行为层次加强网络安全的法律治理。除自然因素等原因外，网络安全事件的爆发往往都是由于相关主体消极进行安全管理或故意实施攻击破坏等行为导致。例如因保密管理不到位导致的网上泄密、恶意网络攻击导致系统崩溃和软硬件故障、借助病毒和木马进行网络商业窃密或给文件加密实施勒索等。利用网络空间散布传播与主流意识形态和公序良俗相背离的煽动性、虚假性言论，均是不负责行为或恶意行为的结果。实施网络安全的法律治理，需要综合运用各种法律工具对危害网络安全的行为进行有效约束，明确网络空间行为的安全便捷，以减少乃至杜绝此类行为的发生。一方面需要对网络活动中

的各类行为进行正面引导，以提倡性规范或强制性规范明确符合网络安全要求的行为模式和安全规范，确立合法安全用网的行为指南；另一方面需要以严格的法律责任对危害网络安全的行为进行否定性评价，完善涵盖民事、行政和刑事责任的法律责任体系，加大对于危害网络安全行为的查处和追责力度。

构建和完善网络安全法律治理体系，在法治框架下应对网络安全这一全球性挑战，是提升我国网络空间治理能力的内在要求，也是我国建设网络强国的重要保障，也是维护我国整体国家安全的应有之义。网络安全法律治理体系是一项系统工程，我们需要以整体性和系统性的思维，在尊重技术规律和法治规律的基础上，精准厘清法律治理体系的层次结构，从基础设施、主体、内容、行为等四个层次为法律治理找到着力点和落脚点，从而构建起全面、科学、有效的网络安全法律治理体系。

袁 康

目 录

第一章 网络安全的体系界定与法律治理机制	1
一、网络安全中的“网络”及相关概念	1
(一) 网络、互联网、信息网络的概念辨析	1
(二) 网络、互联网、信息网络的立法选择	5
(三) 未来网络	7
(四) 智慧社会与智慧网络	11
二、网络安全的体系界定	13
(一) 网络安全与网络空间安全、信息安全的区分	13
(二) 网络安全的立法界定	15
(三) 多维视域下的网络安全的体系界定	16
三、网络安全形势及其法律治理要求	25
(一) 网络安全形势	25
(二) 网络安全的法律治理要求	29
四、网络安全的法律治理机制	31
(一) 网络安全的法律治理机制的指导思想	31
(二) 网络安全的法律治理机制的基本理念	34
(三) 网络安全的法律治理机制的目标和基本内容	38
(四) 网络安全的法律治理机制的进路：技术与法律耦合	39
五、网络安全的法律治理体系	42
(一) 网络安全的法律治理体系的基础框架	42

(二) 《网络安全法》与相关立法的协同治理	45
(三) 网络安全的法律治理的结构与机理	50
(四) 网络安全的国际法律治理机制	52
第二章 网络安全法律与政策的全球实践	62
一、全球网络安全发展的整体检视	63
(一) 全球网络安全发展的现状	63
(二) 全球网络安全发展的背景	68
(三) 全球网络安全发展的威胁	71
二、美洲网络安全治理的实践发展	74
(一) 美国网络安全政策与立法	74
(二) 加拿大网络安全政策与立法	81
三、欧洲网络安全的实践发展	84
(一) 欧盟网络安全政策与立法	84
(二) 德国网络安全政策与立法	86
(三) 英国网络安全政策与立法	88
四、国际组织网络安全的实践发展	91
(一) 联合国网络安全实践发展情况	91
(二) 北大西洋公约组织	95
五、全球网络安全实践发展的困难与应对	98
(一) 发展困难	98
(二) 发展应对	103
第三章 网络运营者的安全保障义务	109
一、网络运营者安全保障义务的基本界定	110
(一) 网络运营者的概念及内涵	110
(二) 安全保障义务的法律性质及基本内容	114
二、网络运营者安全保障义务的适用局限与实现困境	119
(一) 网络运营者安全保障义务的私法适用局限	119
(二) 网络运营者安全保障义务的公法实现困境	123

三、网络运营者安全保障义务的域外法考察及其经验借鉴·····	127
(一) 网络运营者安全保障义务的域外立法考察·····	127
(二) 网络运营者安全保障义务域外立法对我国的启示及借鉴·····	133
四、网络运营者安全保障义务的制度完善·····	135
(一) 制度完善的前提：价值定位与基本立场·····	135
(二) 网络运营者安全保障义务体系协调·····	136
(三) 网络运营者安全保障义务的路径选择·····	139
(四) 网络运营者安全保障义务的配套制度安排·····	143
第四章 网络安全治理中的政府定位与监管机制·····	146
一、网络安全观的滥觞与价值追求·····	146
(一) 网络安全治理的发展历程·····	146
(二) 网络安全治理的基本特征·····	152
(三) 网络安全治理的价值追求·····	156
二、网络安全治理中的政府定位·····	160
(一) 政府角色的宏观定位·····	160
(二) 政府角色的中观定位·····	165
(三) 政府角色的微观定位·····	169
三、网络安全治理中监管机制的路径优化·····	174
(一) 完善网络安全立法·····	174
(二) 健全网络安全监管体制·····	178
(三) 加强关键信息基础设施保护·····	181
(四) 优化网络信息安全管理·····	186
(五) 提升监测预警与应急处置能力·····	189
(六) 加强国际交流与合作·····	192
第五章 行业协会在网络安全治理中的法律地位·····	195
一、行业协会参与网络安全治理的法理逻辑·····	196
(一) 网络安全由单一治理走向综合治理的治道变革·····	196
(二) 行业协会的法律属性与网络安全治理的内在契合·····	199

二、行业协会参与网络安全治理的现状考察·····	202
(一) 行业协会参与网络安全治理的立法现状·····	202
(二) 行业协会参与网络安全治理的实践现状·····	207
(三) 行业协会参与网络安全治理的问题评析·····	212
三、行业协会参与网络安全治理的域外经验·····	221
(一) 美国网络安全治理中的行业自律 ——以美国在线隐私联盟为例·····	223
(二) 英国网络安全治理中的行业自律 ——以网络观察基金为例·····	224
(三) 德国网络安全治理中的行业自律 ——“受规制的自我规制”模式·····	226
(四) 日本网络安全治理中的行业自律 ——“官民合作”治理模式·····	228
(五) 域外经验对我国行业协会参与网络安全治理的启示·····	229
四、行业协会参与网络安全治理的制度完善·····	231
(一) 完善行业协会参与网络安全治理的立法·····	232
(二) 推动行业协会法人治理结构的变革·····	234
(三) 健全行业协会参与网络安全治理的自律机制·····	236
(四) 加强行业协会参与网络安全治理的外部监督·····	238
(五) 构建行业协会与相关主体的网络安全治理合作机制·····	239
第六章 网络基础设施的安全保障及其法律治理·····	244
一、总体国家安全观视域下的网络与网络基础设施·····	245
(一) 总体国家安全观对“网络”与“网络基础设施”的要求·····	245
(二) “网络基础设施安全”治理的物质基础与价值表达·····	247
(三) “网络基础设施安全”相关的制度考察与发展方向判断·····	252
二、网络基础设施的技术分野与安全挑战·····	261
(一) 以网络基础设备为对象的传统安全检视·····	261
(二) 以网络底层数据为对象的网络信息安全保护·····	264
(三) 以“黑箱化”算法为对象的网络逻辑监管·····	265

(四) 以 5G 网络通信技术为代表的未来网络安全关切	267
三、我国网络基础设施安全风险应对策略的理论分析	271
(一) 对传统安全风险线上演进与线下蔓延的警惕	271
(二) 对网络底层数据保护的重视	272
(三) 对网络基础运行逻辑风险的防范	276
(四) 对全球视野下的 5G 网络通信网络的安全预判	277
四、我国网络基础设施治理相关体系的完善	283
(一) 理论层面：以全球网络资源合理分配为价值导向	283
(二) 实践层面：构建网络基础设施安全保障的系统化治理体系	287
第七章 数据安全与个人信息保护的法律治理	296
一、数据安全与个人信息保护的内涵厘清	296
(一) 大数据、数据安全与个人信息	296
(二) 个人信息权	300
二、数据安全与个人信息保护法律治理面临的挑战	304
(一) 个人信息侵权现状的挑战	304
(二) 个人信息立法滞后的挑战	310
(三) 传统司法规则滞后的挑战	317
(四) 数据主权备受冲击的挑战	322
(五) 国际合作安全困境的挑战	324
三、数据安全与个人信息保护法律治理的基本框架	328
(一) 数据安全与个人信息保护法律治理的目标	328
(二) 数据安全与个人信息保护法律治理的原则	330
(三) 数据安全与个人信息保护法律治理的域外经验	334
四、数据安全与个人信息保护法律治理的实现路径	342
(一) 数据安全与个人信息保护法律治理的路径	342
(二) 数据安全与个人信息保护法律治理体系	344
(三) 数据安全与个人信息保护法律治理的具体措施	346
第八章 网络攻击行为的法律规制	353
一、网络攻击行为的类型与形势	354

(一) 技术手段视角下的网络攻击类型	354
(二) 网络攻击行为的层次	357
(三) 网络攻击形势及其对网络安全的挑战	364
二、网络攻击行为发生的原因	367
(一) 违法成本与收益反差巨大	367
(二) 安全漏洞普遍存在	369
三、网络攻击行为治理的法律框架	371
(一) 实然层面	371
(二) 应然层面	376
四、攻击端治理	380
(一) 黑客攻击的动机分析	380
(二) 黑客攻击的一般流程	381
(三) 源头治理黑客攻击行为	382
五、防御端治理	385
(一) 个人终端	385
(二) 企业终端	387
(三) 关键信息基础设施运营者	390
(四) 互联网安全厂商	393
六、体系化治理	395
(一) 技术保障	395
(二) 行业自律	397
(三) 行政管理	398
(四) 社会监督	400
(五) 司法执行	402
第九章 总体国家安全观视野下网络泄密的法律治理	404
一、国家秘密视野下的网络泄密	405
(一) 保密维度下的网络安全	405
(二) 网络安全与国家秘密安全	406
(三) 网络安全与网络平台数据安全	407

二、总体国家安全观对网络泄密法律治理的统领	409
(一) 总体国家安全观的把握重点	409
(二) 网络环境下国家秘密泄露的主要特征	410
(三) 网络平台数据泄露的主要特征	416
(四) 总体国家安全观指导下网络泄密法律治理的基本原则	422
三、积极预防引起核心国家秘密泄露的内部风险	425
(一) 核心国家秘密重点保护的必要性分析	425
(二) 网络安全语境下核心国家秘密泄露危险及法律预防现状	430
(三) 加大引起核心国家秘密泄露危险行为刑法治理力度的 合理性	435
(四) 引起核心国家秘密泄露危险行为刑法治理的立法建议	439
(五) 基于网络运行安全的泄密监督管理过失责任追究	443
四、合理控制网络平台数据泄露犯罪的收益与成本	449
(一) 降低网络平台数据泄露犯罪的收益：控制网络平台数据的 再利用价值，打击下游犯罪	450
(二) 提高网络平台数据泄露犯罪的“投资性”成本：强化网络平台 数据保护责任，打击上游犯罪	454
(三) 提高网络平台数据泄露犯罪的“惩罚性”成本：增强网络平台 数据泄露监测预警和有关部门的技术侦查能力	458
第十章 网络交易安全的法际协调与制度创新	461
一、网络交易安全保障的领域法诉求：以《电子商务法》为中心	462
(一) 网络交易安全法律述评：视阈局限与规则不足	463
(二) 《电子商务法》保障网络交易安全的乏力	470
(三) 经济法保障网络交易安全之规则缺位	479
(四) 网络交易安全保障的领域法思维	481
二、网络交易安全的实体制度保障——以网络教育资源交易为中心	483
(一) 网络教育资源交易及其信息安全问题	483
(二) 网络教育资源交易的信息泄露及保护难题	487
(三) 网络教育资源交易信息的权利化塑造	495

(四) 网络教育资源交易的个人信息安全保护	501
(五) 网络教育资源交易平台的信息安全法律规制	506
三、网络安全的程序制度保障——以社会保险费征管安全为中心	511
(一) 社保费征管信息安全的整体化检视	514
(二) 社保费征管信息的理念导向：从稽征经济到信息安全	520
(三) 社保费征管信息安全保障的法治进路	529
后记	541

第一章

网络安全的体系界定与 法律治理机制

网络安全的法律治理的前提是明确何为网络安全，然而，在立法和相关研究中，关于网络安全存在不同的认识，甚至是误用，以致用语不一和概念不清，这直接影响了网络安全立法未能对网络安全提供足够的法律供给。因此，需要对网络安全进行体系化界定，从而为构建科学、合理、可行的网络安全法律治理机制奠定基础。

一、网络安全中的“网络”及相关概念

概念是逻辑的起点，也是研究的基本要素。要探讨网络安全及其体系界定，首先需要对网络、网络安全及相关的概念进行辨析性界定。

（一）网络、互联网、信息网络的概念辨析

1. “四网融合”语境下的网络、互联网、信息网络

“网络”一词可以用于很多地方，例如社群网络、销售网络、交通网络等。互联网来到我国以后就常被简称为“网络”，随着互联网的兴起，日常生活中的“网络”一词往往指向互联网。虽然互联网和 EDI（电子数据交换）网络等都属于互联网，但由于互联网是最主要的，在很多语境中，网络就是指互联网。在我国，与互联网并列的网络还有电信网和广播电视网。由于“三网融合”的深入发展，三网之间在技术与应用方面已经不存在实质性的区别。例如，借助互联网实现的网络广播电视和网络电话等新应用和新功能，利用广播