

上海交通大学网络空间治理研究中心学术文库
上海交通大学中央高校基本科研业务费资助项目

中国科学技术法学会网络空间法专业委员会组织编写
网络空间治理前沿研究丛书

网络安全法 实用教程

主编 寿步



上海交通大学出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

上海交通大学网络空间治理研究中心学术文库
上海交通大学中央高校基本科研业务费资助项目

网络安全法实用教程

主 编 寿 步
副主编 秦 倩 党玉洁

撰稿人
寿 步 秦 倩 党玉洁
吴佳佳 张 玥 廖小其



上海交通大学出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

内容提要

本书是在全面收集整理网络安全法发布以来的相关规范性文件的基础上,按照网络安全法的制度设计进行章节划分,针对实务需要编撰的教材。本书分为十章,包括网络安全法导读、网络安全法总则、网络安全支持与促进制度、网络运行安全制度的一般规定、关键信息基础设施运行安全制度、个人信息保护制度、违法信息监管制度、数据出境管理制度、网络安全监测预警与应急处置制度、网络安全法律责任制度。本书的内容取材于规范性文件,权威性高,实用性强,方便实务学习。本书可供关心网络安全和网络安全法的读者阅读,也可供网络安全法实务培训使用。

图书在版编目(CIP)数据

网络安全法实用教程 / 寿步主编. —上海:上海交通大学出版社,2019

ISBN 978 - 7 - 313 - 22736 - 2

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

中国版本图书馆CIP数据核字(2019)第282650号

网络安全法实用教程

WANGLUO ANQUANFA SHIYONG JIAOCHENG

主 编:寿 步

出版发行:上海交通大学出版社

邮政编码:200030

印 刷:常熟市文化印刷有限公司

开 本:710mm×1000mm 1/16

字 数:297千字

版 次:2019年12月第1版

书 号:ISBN 978 - 7 - 313 - 22736 - 2

定 价:78.00元

副 主 编:党玉洁 秦 倩

地 址:上海市番禺路951号

电 话:021 - 64071208

经 销:全国新华书店

印 张:14.5

印 次:2019年12月第1次印刷

版权所有 侵权必究

告 读 者:如发现本书有印装质量问题请与印刷厂质量科联系

联系电话:0512 - 52219025

前 言

一、缘起

20世纪90年代以来,信息技术在全球迅速发展,互联网在各国广泛应用,使得人类社会各领域发生了深刻变化,极大地改变和影响人们的社会活动和生活方式。网络与信息技术的应用,在促进技术创新、经济发展、文化繁荣、社会进步的同时,也导致网络安全问题日益凸显。在此背景下,应对来自网络空间的安全挑战,切实保障网络空间安全,已经成为各国面临的共同课题。互联网的全球性,导致网络空间的安全问题必然也是全球性、综合性的社会问题。网络空间的安全问题,首先离不开法律的规制。

2014年2月,由习近平总书记任组长的中共中央网络安全和信息化领导小组的成立,将网络安全提升到国家战略的重要地位,对加强国家网络安全工作作出重要部署,要求完善网络安全保护方面的法律法规。在此背景下,2016年11月7日全国人大常委会通过《中华人民共和国网络安全法》(以下简称“网络安全法”)。我国现已进入以网络安全法为统领、以《国家网络空间安全战略》为指导、构建网络安全法律全面保障体系的新时期。

因此,加强网络安全立法研究,推动建立健全我国网络安全法律体系,不仅对健全我国法律体系具有重要的理论意义,而且对维护国家安全、保障社会经济科技文化发展具有重要的现实意义。

笔者在主持上海交通大学中央高校基本科研业务费资助项目《网络空间安全法律问题研究》期间,制订“网络安全法三部曲”的编撰出版计划。此前已经出版了两本书。

2017年出版的《网络安全法实务指南》,是在全面收集整理当时我国与网络安全相关的规范性文件基础上,以《中华人民共和国网络安全法》的章节条款为主线,分解设立法律问题,按问答形式整理形成的网络安全法律政策汇编,方便读者检索问题,找到答案。

2018年出版的《网络空间安全法律问题研究——基于ISO/IEC 27032:2012的视角》,是网络空间安全法律体系的理论研究成果。该书提出:如果以ISO/IEC 27032:2012为基础制定我国网络空间安全法,则既可以使法律本身建立在严谨、

周密、坚实的技术基础上,给法律规制未来出现在网络空间中的新问题预留空间,也有助于建立科学的、完整的网络空间安全法学理论体系。

这本《网络安全法实用教程》是“网络安全法三部曲”中的第三本书。

二、概要

2017年6月1日网络安全法施行以来,国家主管机关颁布了与网络安全法配套或相关的一系列法律、行政法规、部门规章、司法解释、国家标准、行业标准或其征求意见稿;司法机关对涉及网络安全的一系列民事、刑事、行政案件进行了裁判;行政机关对涉及网络安全的一系列违法行为进行了行政处罚。

本书的编撰依据是:①我国与网络安全相关的法律、法规、司法解释、部门规章;②我国与网络安全相关的国家标准和行业标准;③前述两类文件的征求意见稿。

在充分收集整理近几年规范性文件和裁判处罚文书的基础上,结合实务工作需要,按照网络安全法的制度设计逻辑进行本书的章节安排,本书分为十章:网络安全法导读,网络安全法总则,网络安全支持与促进制度,网络运行安全制度的一般规定,关键信息基础设施运行安全制度,个人信息保护制度,违法信息管控制度,数据出境管理制度,网络安全监测预警与应急处置制度,网络安全法律责任制度。书后以网络安全法的全文作为附录,以便读者查阅。

本书对我国网络安全法律政策的体系内容和执法实践做了较为全面完整的介绍,可作为网络安全法的培训教材,供所有关心网络安全工作和网络安全法律制度的读者,特别是网络安全法律风险防范与合规的实务工作者阅读参考。

本书的编撰由寿步统筹谋划。寿步和秦倩、党玉洁、吴佳佳、张玥、廖小其参加了本书的撰写,由寿步修改定稿。

本书的资料收集,得到了上海市通力律师事务所合伙人潘永建律师及其团队的大力支持。在此谨致谢忱。

借此机会,对上海交通大学网络安全技术研究院院长、信息内容分析技术国家工程实验室主任、中国网络空间安全协会副理事长李建华教授的宝贵支持致以衷心的感谢;对上海交通大学信息内容分析技术国家工程实验室副主任、网络空间治理研究中心主任潘理研究员的大力合作致以诚挚的谢意。

由于作者水平的限制,本书定有不足之处,欢迎读者批评指正。

寿步

二〇一九年八月

目 录

第一章 网络安全法导读	1
第一节 网络安全法概述	1
第二节 网络安全法术语	5
本章相关规范性文件目录	8
第二章 网络安全法总则	9
第一节 立法目的	9
第二节 适用范围	11
第三节 网络安全与信息化发展并重原则	11
第四节 保障网络安全的战略布局	12
第五节 保障网络安全的规则框架	14
第六节 保障网络安全的监管体系	16
第七节 未成年人网络保护制度	21
第八节 案例介绍	23
本章相关规范性文件目录	27
第三章 网络安全支持与促进制度	30
第一节 推进标准体系建设 支持技术和产业发展	30
第二节 推动社会化服务体系建设 促进数据资源开发利用	33
第三节 开展宣传教育 培养专业人才	37
本章相关规范性文件目录	40
第四章 网络运行安全制度一般规定	42
第一节 网络安全等级保护制度	42
第二节 网络运营者义务	48
第三节 网络产品和服务的安全保障	57
第四节 网络安全服务活动规范	62

第五节 禁止危害网络安全的行为	66
第六节 网络安全合作和执法中获取信息的用途限制	68
第七节 案例介绍	69
本章相关规范性文件目录	73
第五章 关键信息基础设施运行安全制度	79
第一节 建立关键信息基础设施保护制度	79
第二节 关键信息基础设施运营者的义务	84
本章相关规范性文件目录	95
第六章 个人信息保护制度	97
第一节 我国个人信息保护法律体系	97
第二节 个人信息保护制度概述	100
第三节 个人信息的收集、使用规则	107
第四节 个人信息的保存、委托处理、共享、转让、公开披露规则	115
第五节 个人信息的查询、更正、删除规则	125
第六节 儿童个人信息网络保护规定和 App 收集使用个人信息治理 ..	128
第七节 案例介绍	136
本章相关规范性文件目录	140
第七章 违法信息监管制度	143
第一节 违法信息监管制度概述	143
第二节 网络使用者的一般义务	146
第三节 网络运营者处置违法信息的义务	149
第四节 网络运营者建立投诉举报制度的义务	151
第五节 网络运营者配合监督检查的义务	153
第六节 国家对违法信息的监督管理	155
第七节 案例介绍	156
本章相关规范性文件目录	158
第八章 数据出境管理制度	160
第一节 个人信息和重要数据的识别	160
第二节 数据的境内存储	163
第三节 数据的出境评估	165
本章相关规范性文件目录	172

第九章 网络安全监测预警与应急处置制度	174
第一节 网络安全监测预警与信息通报制度的一般规定	174
第二节 关键信息基础设施的监测预警与信息通报制度	178
第三节 网络安全风险预警措施	179
第四节 网络安全应急处置制度	181
第五节 网络安全监督管理约谈制度	187
第六节 突发事件和生产安全事故的处置	189
第七节 网络通信的临时限制措施	193
本章相关规范性文件目录	194
第十章 网络安全法律责任制度	196
第一节 网络安全法律责任的一般规定	196
第二节 网络运行安全制度一般规定的行政责任	197
第三节 关键信息基础设施运行安全制度的行政责任	201
第四节 个人信息保护制度的行政责任	202
第五节 违法信息监管制度的行政责任	205
第六节 数据出境管理制度的行政责任	208
本章相关规范性文件目录	210
附录 中华人民共和国网络安全法	211
参考文献	222

第一章 网络安全法导读

第一节 网络安全法概述

一、立法必要性和起草经过

20世纪90年代以来,信息技术在全球迅速发展,互联网(Internet)在各国广泛应用,使得人类社会各领域发生了深刻变化,极大地改变和影响人们的社会活动和生活方式。网络与信息技术的应用,在促进技术创新、经济发展、文化繁荣、社会进步的同时,也导致网络安全问题日益凸显。

(1)网络入侵、网络攻击等非法活动,严重威胁着电信、能源、交通、金融以及国防军事、行政管理等重要领域的信息基础设施的安全,云计算、大数据、物联网等新技术、新应用面临着更为复杂的网络安全环境。

(2)非法获取、泄露甚至倒卖公民个人信息,侮辱诽谤他人、侵犯知识产权等违法活动在网络上时有发生,严重损害公民、法人和其他组织的合法权益。

(3)宣扬恐怖主义、极端主义,煽动颠覆国家政权、推翻社会主义制度,以及淫秽色情等违法信息,借助网络传播、扩散,严重危害国家安全和社会公共利益。网络安全已成为关系国家安全和发展的,关系人民群众切身利益的重大问题。

在此背景下,应对来自网络空间的安全挑战,切实保障网络空间安全,已经成为各国面临的共同课题。互联网的全球性,导致网络空间的安全问题必然也是全球性综合性的社会问题。网络空间安全问题的解决,当然就离不开法律的规制。

我国网络安全法律制度的历史可以分为两个阶段。

第一阶段,从20世纪90年代到2014年2月中共中央网络安全和信息化领导小组成立。

这一时期我国的网络安全立法基本属于渗透型模式,也就是将涉及网络安全的相关规定渗透融入相关的法律、行政法规、部门规章、司法解释、国家标准、行业标准等规范性文件中,其内容涉及网络监管、信息安全等级保护等多方面。

第二阶段,从2014年2月中共中央网络安全和信息化领导小组成立至今。

2014年2月27日,习近平总书记在中共中央网络安全和信息化领导小组第一次会议上强调,“没有网络安全,就没有国家安全”。中央网络安全和信息化领导小组的成立,极大地推动了各级党委政府和各行各业对网络安全工作的关注和重视,网络安全已经提升到国家战略的重要地位。2014年4月15日,习近平总书记在中央国家安全委员会第一次会议上提出,坚持总体国家安全观,走出一条中国特色国家安全道路。以习近平同志为核心的党中央从总体国家安全观出发,就网络安全问题提出了一系列新思想、新观点、新论断,对加强国家网络安全工作作出重要部署。2014年10月中共十八届四中全会决定要求完善网络安全保护方面的法律法规。

广大人民群众十分关注网络安全,强烈要求依法加强网络空间治理,规范网络信息传播秩序,惩治网络违法犯罪,使网络空间晴朗起来。

为适应国家网络安全工作的新形势和新任务,落实党中央的要求,回应人民群众的期待,第十二届全国人大常委会于2013年10月将制定网络安全方面的立法列入该届全国人大常委会的立法规划,之后又列入2014年至2016年的立法工作计划。

2014年上半年,全国人大常委会法制工作委员会组成工作专班,开展网络安全法研究起草工作。通过召开座谈会、论证会等多种方式听取各方面的意见,并到一些地方调研,深入了解网络安全领域存在的突出问题,掌握各方面的立法需求。在此基础上,先后提出了网络安全立法的基本思路、制度框架和草案初稿,会同中央网络安全和信息化领导小组办公室与工业和信息化部、公安部、原国务院法制办等部门多次交换意见,反复研究,提出了《网络安全法(草案征求意见稿)》。经同中央国家安全委员会办公室、中央网络安全和信息化领导小组办公室共同商量,再次征求有关部门的意见,做了进一步完善,形成了《网络安全法(草案)》,于2015年6月由全国人大常委会委员长会议提请十二届全国人大常委会第十五次会议进行审议。

初次审议之后,网络安全法(草案)印发至各相关机构和部门,并在中国人大网公布,向社会公开征求意见。

2016年6月,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)》进行审议。

二次审议之后,《网络安全法(草案二次审议稿)》在中国人大网公布,向社会公开征求意见。

在此基础上,2016年11月7日,十二届全国人大常委会第二十四次会议审议通过《中华人民共和国网络安全法》。

2018年3月,根据中共中央印发的《深化党和国家机构改革方案》,将中共中央网络安全和信息化领导小组改为中共中央网络安全和信息化委员会,负责相关领域重大工作的顶层设计、总体布局、统筹协调、整体推进、督促落实。

我国现已进入以网络安全法为统领,以《国家网络空间安全战略》为指导,构建网络空间安全法律全面保障体系的新时期。

二、立法指导思想和起草工作要点

网络安全法的指导思想是:坚持以总体国家安全观为指导,全面落实党的十八大和十八届三中、四中全会决策部署,坚持积极利用、科学发展、依法管理、确保安全的方针,充分发挥立法的引领和推动作用,针对当前我国网络安全领域的突出问题,以制度建设提高国家网络安全保障能力,掌握网络空间治理和规则制定方面的主动权,切实维护国家网络空间主权、安全和发展利益。

据此,网络安全法的起草工作把握了以下几点:

第一,坚持从国情出发。根据我国网络安全面临的严峻形势和网络立法的现状,充分总结近年来网络安全工作经验,确立保障网络安全的基本制度框架。重点对网络自身的安全作出制度性安排,同时在信息内容方面也作出相应的规范性规定,从网络设备设施安全、网络运行安全、网络数据安全、网络信息安全等方面建立和完善相关制度,体现中国特色;并注意借鉴有关国家的经验,主要制度与国外通行做法是一致的,并对内外资企业同等对待,不实行差别待遇。

第二,坚持问题导向。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。

第三,坚持安全与发展并重。维护网络安全,必须坚持积极利用、科学发展、依法管理、确保安全的方针,处理好与信息化发展的关系,做到协调一致、齐头并进。通过保障安全为发展提供良好环境,本法注重对网络安全制度作出规范的同时,注意保护各类网络主体的合法权利,保障网络信息依法有序自由流动,促进网络技术创新和信息化持续健康发展。

三、网络安全法的主要内容

网络安全法共有七章,共七十九条。网络安全法全文可见附录《中华人民共和国网络安全法》。与网络安全法各项制度相关的规范性文件,可见本书各章最后的《本章相关规范性文件目录》。

网络安全法的主要内容包括:

(一) 维护网络空间主权

网络空间主权是国家主权在网络空间的体现和延伸,网络空间主权原则是我国维护国家安全和利益、参与网络空间国际治理与合作所坚持的重要原则。为此,网络安全法将“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”作为立法

宗旨,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”。

(二) 保障网络产品和服务安全

维护网络安全,首先要保障网络产品和服务的安全。网络安全法明确了网络产品和服务提供者的安全义务;规定了网络产品和服务提供者的个人信息保护义务;将网络关键设备和网络安全专用产品的安全认证和安全检测制度上升为法律并作了必要的规范;对网络安全服务活动作了原则规范。

(三) 保障网络运行安全

保障网络运行安全,必须落实网络运营者第一责任人的责任。据此,网络安全法将此前实行的网络安全等级保护制度上升为法律,要求网络运营者按照网络安全等级保护制度的要求,采取相应的管理措施和技术防范等措施,履行相应的网络安全保护义务。

(四) 保障关键信息基础设施安全

为了保障关键信息基础设施安全,维护国家安全、经济安全和保障民生,网络安全法设专节对关键信息基础设施的运行安全作了规定,实行重点保护。对关键信息基础设施的范围、关键信息基础设施保护制度的主要内容、关键信息基础设施的运营者采购网络产品和服务的国家安全审查措施、关键信息基础设施的数据的境内存储和跨境提供作了原则规定。

(五) 个人信息保护

在2012年全国人大常委会《关于加强网络信息保护的決定》基础上,网络安全法进一步完善了网络运营者收集使用个人信息的规则、网络运营者保护个人信息的义务与责任,加强对个人信息的保护,防止个人信息数据被非法获取、泄露或者非法使用。

(六) 保障网络信息安全

在2012年全国人大常委会《关于加强网络信息保护的決定》基础上,网络安全法进一步完善了保障网络信息安全的規定。一是确立了网络身份管理制度即网络实名制,以保障网络信息的可追溯;二是明确了网络运营者处置违法信息的义务;三是規定了发送电子信息、提供应用软件不得含有法律和行政法规禁止发布或者传输的信息;四是規定了网络运营者应当为公安机关、国家安全机关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;五是赋予有关主管部门处置违法信息、阻断违法信息传播的权力。

(七) 监测预警与应急处置

为了加强国家的网络安全监测预警和应急制度建设,提高网络安全保障能力,网络安全法規定:一是国家建立网络安全监测预警和信息通报制度,加强网络安全信息收集、分析和情况通报工作;二是建立健全重要行业、重要领域的网络安全监测预警和信息通报制度;三是規定了政府部门网络安全信息的监测、分析、预警制

度和网络安全事件的应急处置措施；四是规定了为维护国家安全和社会公共秩序，处置重大突发社会安全事件的网络通信临时限制措施。

（八）网络安全监督管理体制

为加强网络安全工作，网络安全法规定由国家网信部门对网络安全工作的统筹协调职责和相关监督管理职责，同时规定了国务院电信主管部门、公安部门和其他有关机关以及地方政府有关部门的网络安全监督管理职责。

（九）法律责任

网络安全法对于不履行网络安全法关于网络运行安全制度的一般规定、关键信息基础设施运行安全制度规定、个人信息保护制度规定、违法信息监管制度规定、数据出境管理制度规定的法律责任，也作了明确规定。

（十）其他

网络安全法第七章附则包含第七十六条至第七十九条，规定了其他事项。

网络安全法第七十六条对本法相关术语如网络、网络安全、网络运营者、网络数据、个人信息等作出定义。

针对涉密网络的运行安全，网络安全法第七十七条规定：“存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。”

军事网络是中华人民共和国武装力量管理和指挥作战系统的重要组成部分，与民用网络相比，有其特殊性。军事网络面临的安全威胁也日益凸显。网络安全法第七十八条规定：“军事网络的安全保护，由中央军事委员会另行规定。”

关于施行日期，网络安全法第七十九条规定：“本法自2017年6月1日起施行。”

第二节 网络安全法术语

在网络安全法以及与网络安全相关的规范性文件中，包含对网络安全相关术语的定义。给出定义的包括但不限于下列术语。

一、网络

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。（网络安全法第七十六条）

二、网络安全

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。(网络安全法第七十六条)

三、网络运营者

网络运营者,是指网络的所有者、管理者和网络服务提供者。(网络安全法第七十六条)

四、网络信息服务提供者

网络信息服务提供者,是指通过网络向用户提供信息技术、信息服务、信息产品的组织和个人,包括网络平台服务提供者、网络内容及产品服务提供者。(《未成年人网络保护条例(送审稿)》第三十五条)

五、网络数据

网络数据,是指通过网络收集、存储、传输、处理和产生的各种电子数据。(网络安全法第七十六条)

六、个人信息及相关术语

(1)个人信息(personal information),是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息,包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。(网络安全法第七十六条)

刑法第二百五十三条之一规定的“公民个人信息”,是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息,包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。(《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第一条)

个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。(注:个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。)(GB/T 35273—2017《信息安全技术 个人信息安全规范》3.1)

(2)个人敏感信息(personal sensitive information),是指一旦泄露、非法提供或滥用可能危害人身和财产安全,极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。(注:个人敏感信息包括身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14岁以下(含)儿童的个人信息等。)(GB/T 35273—2017《信息安全技术 个人信息安全规范》3.2)

个人敏感信息,是指一旦被泄露、窃取、篡改、非法使用可能危害个人信息主体人身、财产安全,或导致个人信息主体名誉、身心健康受到损害等的个人信息。(《个人信息出境安全评估办法(征求意见稿)》第二十一条)

(3)个人信息主体(personal data subject),是指个人信息所标识的自然人。(GB/T 35273—2017《信息安全技术 个人信息安全规范》3.3)

个人信息主体,是指个人信息所标识或关联到的自然人。(《数据安全管理办法(征求意见稿)》第三十八条)

(4)个人信息控制者(personal data controller),是指有权决定个人信息处理目的、方式等的组织或个人。(GB/T 35273—2017《信息安全技术 个人信息安全规范》3.4)

(5)未成年人个人信息,是指以电子或者其他方式记录的能够单独或与其他信息结合识别未成年人身份的各种信息,包括但不限于未成年人的姓名、位置、住址、出生日期、联系方式、账号名称、身份证件号码、个人生物识别信息、肖像等。(《未成年人网络保护条例(送审稿)》第三十五条)

七、重要数据

重要数据,是指与国家安全、经济发展,以及社会公共利益密切相关的数据,具体范围参照国家有关标准和重要数据识别指南。(《个人信息和重要数据出境安全评估办法(征求意见稿)》第十七条)

八、数据出境

数据出境,是指网络运营者将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,提供给位于境外的机构、组织、个人。(《个人信息和重要数据出境安全评估办法(征求意见稿)》第十七条)

九、网络安全事件

网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等,对网络和信息系统或者其中的数据造成危害,对社会造成负面影响的事件,可分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他事件。(《国家网络安全事件应急预案》1.3)

十、网络运行事故

网络运行事故是指由于突发公共事件、人为破坏、施工损坏或网络自身故障造成的电信基础设施损坏、电信网络中断、电信业务中断等情况。分为特别重大事故、重大事故、较大事故和一般事故。(《电信网络运行监督管理办法》第三条)

本章相关规范性文件目录

(按发布时间排序)

1. 工业和信息化部《电信网络运行监督管理办法》2009.04.24 发布、2009.05.01 实施
2. 《全国人民代表大会常务委员会关于加强网络信息保护的決定》2012.12.28 发布、实施
3. 国家互联网信息办公室《国家网络空间安全战略》2016.12.27 发布、实施
4. 国务院法制办公室《未成年人网络保护条例(送审稿)》2017.01.06 发布
5. 中央网络安全和信息化领导小组办公室《国家网络安全事件应急预案》2017.01.10 发布、实施
6. 国家互联网信息办公室《个人信息和重要数据出境安全评估办法(征求意见稿)》2017.04.11 发布
7. 《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》2017.05.08 发布、2017.06.01 实施
8. 国家质量监督检验检疫总局、国家标准化管理委员会 GB/T 35273—2017《信息安全技术 个人信息安全规范》2017.12.29 发布、2018.05.01 实施
9. 国家互联网信息办公室《数据安全管理办法(征求意见稿)》2019.05.28 发布
10. 国家互联网信息办公室《个人信息出境安全评估办法(征求意见稿)》2019.06.13 发布

第二章 网络安全法总则

网络安全法第一章总则包含第一条至第十四条,主要涉及网络安全法的立法目的和适用范围、网络安全与信息化发展并重原则、保障网络安全的战略布局、保障网络安全的规则框架、保障网络安全的监管体系、未成年人网络保护制度等。本章对此进行讨论。

第一节 立法目的

关于立法目的,网络安全法第一条规定:“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。”

一、保障网络安全

网络安全法是我国网络安全领域的基础性法律。保障网络安全是制定本法的首要目的。网络安全法涉及网络运行安全制度和网络信息安全制度,其中网络运行安全制度既包括网络安全等级保护制度等一般制度,也包括关键信息基础设施运行安全制度,网络信息安全制度包括个人信息保护制度、违法信息监管制度、数据跨境传输制度。网络安全法还涉及网络安全支持与促进制度、网络安全监测预警与应急处置制度、网络安全法律责任制度等。

二、维护网络空间主权

网络空间主权是国家主权在网络空间的延伸和表现。《国家安全法》第二十五条规定:“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。”这是我国法律首次涉及“网络空间主权”的概念。网络安全法以“维护网络空间主权”为立法目的之一,为我国网络空间主权的行使